PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-185501

(43)Date of publication of application : 15.07.1997

(51)Int.Cl. G06F 9/06
G09C 1/00

(21)Application number : 07-343820

(22)Date of filing : 28.12.1995

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

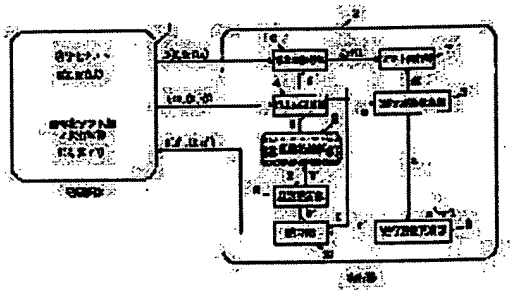
(72)Inventor : MATSUZAKI NATSUME

(54) SOFTWARE EXECUTION CONTROL SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a software execution control system which executes software obtained by means of executing decoding with a software key and prevents the illegal use of the software key and the frequencies of execution when the frequency of execution satisfies a prescribed condition.

SOLUTION: An execution unit 2 stores random numbers in a random number storage part 3 where reading and writing are difficult and a recording medium 1 stores ciphering software and ciphering software key execution frequencies. The execution unit 2 acquires the ciphering software key execution frequencies decodes them with the random numbers, decodes ciphering software with the software key, and executes software when the execution frequency satisfies the prescribed condition. The execution unit 2 updates the execution frequencies and the random numbers, ciphers the software key and the updated number of execution times with the updated random numbers and stores them in the recording medium 1. Thus, the copied ciphering software key execution frequency cannot be decoded by updating the random numbers whenever software is executed.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平9－185501

(43)公開日　平成９年(1997)７月15日

(51)Int.Cl.⁶		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	9/06	５５０		Ｇ０６Ｆ	9/06	５５０Ｂ
Ｇ０９Ｃ	1/00	６３０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６３０Ｅ

審査請求　未請求　請求項の数24　ＯＬ　（全 22 頁）

(21)出願番号　特願平7－343820

(22)出願日　平成７年(1995)12月28日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　松崎　なつめ
大阪府門真市大字門真1006番地　松下電器産業株式会社内

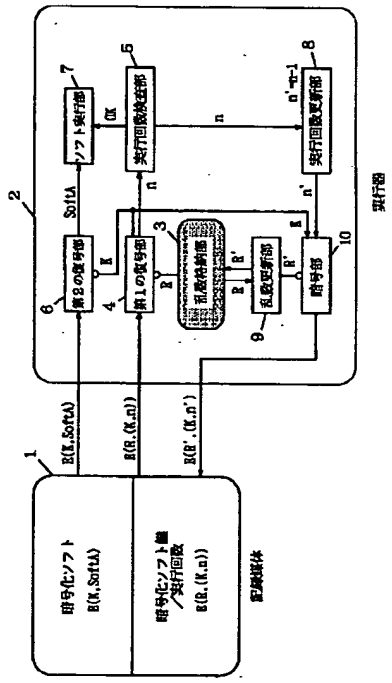
(74)代理人　弁理士　小笠原　史朗

(54)【発明の名称】　ソフトウェア実行制御システム

(57)【要約】

【課題】　実行回数が所定の条件を満足する場合に、ソフト鍵で復号して得られたソフトウェアを実行し、かつ、ソフト鍵および実行回数の不正な使用を防止するソフトウェア実行制御システムを提供する。

【解決手段】　実行器２は、読み出しおよび書き込みが困難な乱数格納部３に乱数を格納し、記録媒体１は、暗号化ソフトウェアおよび暗号化ソフト鍵／実行回数を格納している。実行器２は、記録媒体１から暗号化ソフト鍵／実行回数を獲得して乱数で復号し、次にソフト鍵で暗号化ソフトウェアを復号し、実行回数が所定の条件を満足すればソフトウェアを実行する。続いて実行器２は、実行回数と乱数とを更新し、更新した乱数によって、ソフト鍵および更新した実行回数を暗号化して記録媒体１に格納する。ソフトウェアの実行毎に乱数の更新を行うことで、コピーされた暗号化ソフト鍵／実行回数を復号不能にすることができる。



【特許請求の範囲】
【請求項１】　予め定められた実行許可情報に従ってソフトウェアの実行を制御し、かつ当該実行許可情報の不正な使用を防止するためのソフトウェア実行制御システムであって、
ソフトウェアおよび暗号化された実行許可情報を格納し、かつ情報の読み出しおよび書き込みが可能な記録媒体が、ソフトウェアを実行する実行器に情報伝達可能に接続され、
前記実行器は、
乱数を格納し、かつ自己の外部からは情報の読み出しおよび書き込みが困難な乱数格納手段と、
前記記録媒体から暗号化された実行許可情報を獲得して、前記乱数格納手段から取得した乱数で復号する復号手段と、
前記記録媒体からソフトウェアを獲得して、前記復号手段の復号によって得られた実行許可情報に従って実行するソフト実行手段と、
ソフトウェアの実行に関連して、前記乱数格納手段に格納された乱数を更新する乱数更新手段と、
前記復号手段の復号によって得られた実行許可情報を、前記ソフト実行手段がソフトウェアを実行した後に、前記乱数更新手段によって更新された乱数で暗号化して、前記記録媒体に格納する暗号化手段とを備える、ソフトウェア実行制御システム。
【請求項２】　ソフトウェアの実行にともなって、前記復号手段の復号によって得られた実行許可情報を更新する実行許可情報更新手段をさらに備え、
前記暗号化手段は、前記実行許可情報更新手段によって更新された実行許可情報を、前記乱数更新手段によって更新された乱数で暗号化して、前記記録媒体に格納することを特徴とする、請求項１に記載のソフトウェア実行制御システム。
【請求項３】　前記乱数更新手段は、ソフトウェアの実行毎に、前記乱数格納手段に格納された乱数を更新することを特徴とする、請求項１または２に記載のソフトウェア実行制御システム。
【請求項４】　前記乱数更新手段は、予め決められた複数回のソフトウェアの実行に一度、前記乱数格納手段に格納された乱数を更新することを特徴とする、請求項１または２に記載のソフトウェア実行制御システム。
【請求項５】　前記乱数更新手段は、予め決められた可変の回数のソフトウェアの実行に一度、前記乱数格納手段に格納された乱数を更新し、
乱数の更新の間隔に関する情報を、ソフトウェア使用者に秘密にすることを特徴とする、請求項１または２に記載のソフトウェア実行制御システム。
【請求項６】　前記乱数格納手段は、前記実行器に設けられる代わりに、前記記録媒体に設けられることを特徴とする、請求項１または２に記載のソフトウェア実行制御システム。
【請求項７】　前記記録媒体の代わりに、読み出し専用の第１の記録媒体と、読み出しおよび書き込みが可能な第２の記録媒体とが前記実行器に接続され、
前記第１の記録媒体はソフトウェアを格納し、前記第２の記録媒体は暗号化された実行許可情報を格納することを特徴とする、請求項１または２に記載のソフトウェア実行制御システム。
【請求項８】　前記記録媒体に格納されたソフトウェアは、暗号化されており、
前記ソフト実行手段は、前記記録媒体から暗号化されたソフトウェアを獲得して、前記復号手段の復号によって得られた実行許可情報に従って復号し、復号して得たソフトウェアを実行することを特徴とする、請求項１または２に記載のソフトウェア実行制御システム。
【請求項９】　予め定められた実行許可情報に従ってソフトウェアの実行を制御し、かつ当該実行許可情報の不正な使用を防止するためのソフトウェア実行制御システムであって、
複数の、ソフトウェア、暗号化された実行許可情報および暗号化された補助鍵を格納し、かつ情報の読み出しおよび書き込みが可能な記録媒体が、ソフトウェアを実行する実行器に情報伝達可能に接続され、
前記実行器は、
乱数を格納し、かつ自己の外部からは情報の読み出しおよび書き込みが困難な乱数格納手段と、
前記記録媒体から暗号化された補助鍵を獲得して、前記乱数格納手段から取得した乱数で復号する第１の復号手段と、
前記記録媒体から暗号化された実行許可情報を獲得して、前記第１の復号手段の復号によって得られた補助鍵で復号する第２の復号手段と、
前記記録媒体から対応するソフトウェアを獲得して、前記第２の復号手段の復号によって得られた実行許可情報に従って実行するソフト実行手段と、
前記第２の復号手段の復号によって得られた実行許可情報を、前記ソフト実行手段がソフトウェアを実行した後に、前記第１の復号手段の復号によって得られた補助鍵で暗号化して、前記記録媒体に格納する第１の暗号化手段と、
ソフトウェアの実行に関連して、前記記録媒体から全ての暗号化された補助鍵を獲得して、前記乱数格納手段に格納された乱数で復号する第３の復号手段と、
前記第３の復号手段の復号に連携して、前記乱数格納手段に格納された乱数を更新する乱数更新手段と、
前記第３の復号手段の復号によって得られた補助鍵を、前記乱数更新手段によって更新された乱数で暗号化して、前記記録媒体に格納する第２の暗号化手段とを備える、ソフトウェア実行制御システム。
【請求項１０】　ソフトウェアの実行にともなって、前

記第２の復号手段の復号によって得られた実行許可情報を更新する実行許可情報更新手段をさらに備え、
前記第１の暗号化手段は、前記実行許可情報更新手段によって更新された実行許可情報を、前記第１の復号手段の復号によって得られた補助鍵で暗号化して、前記記録媒体に格納することを特徴とする、請求項９に記載のソフトウェア実行制御システム。
【請求項１１】　前記第３の復号手段は、ソフトウェアの実行毎に、前記記録媒体から全ての暗号化された補助鍵を獲得して、前記乱数格納手段に格納された乱数で復号することを特徴とする、請求項９または１０に記載のソフトウェア実行制御システム。
【請求項１２】　前記第３の復号手段は、予め決められた複数回のソフトウェアの実行に一度、前記記録媒体から全ての暗号化された補助鍵を獲得して、前記乱数格納手段に格納された乱数で復号することを特徴とする、請求項９または１０に記載のソフトウェア実行制御システム。
【請求項１３】　前記第３の復号手段は、予め決められた可変の回数のソフトウェアの実行に一度、前記記録媒体から全ての暗号化された補助鍵を獲得して、前記乱数格納手段に格納された乱数で復号し、
暗号化された補助鍵の復号の間隔に関する情報をソフトウェア使用者に秘密にすることを特徴とする、請求項９または１０に記載のソフトウェア実行制御システム。
【請求項１４】　前記乱数格納手段は、前記実行器に設けられる代わりに、前記記録媒体に設けられることを特徴とする、請求項９または１０に記載のソフトウェア実行制御システム。
【請求項１５】　前記記録媒体の代わりに、読み出し専用の第１の記録媒体と、読み出しおよび書き込みが可能な第２の記録媒体とが前記実行器に接続され、
前記第１の記録媒体はソフトウェアを格納し、前記第２の記録媒体は暗号化された実行許可情報を格納し、
前記乱数格納手段は、前記実行器に設けられる代わりに、前記第２の記録媒体に設けられることを特徴とする、請求項９または１０に記載のソフトウェア実行制御システム。
【請求項１６】　前記記録媒体に格納されたソフトウェアは、それぞれ暗号化されており、
前記ソフト実行手段は、前記記録媒体から、対応する暗号化されたソフトウェアを獲得して、前記第２の復号手段の復号によって得られた実行許可情報に従って復号し、復号して得たソフトウェアを実行することを特徴とする、請求項９または１０に記載のソフトウェア実行制御システム。
【請求項１７】　ソフトウェアを実行する実行器と、当該実行器に情報伝達可能に接続され、かつ情報の読み出しおよび書き込みが可能な記録媒体と、実行器の求めに応じて実行許可情報を配布するソフト配布器とからなり、ソフト配布器から配布される実行許可情報の不正な使用を防止するためのソフトウェア実行制御システムであって、
前記ソフト配布器は、実行許可情報を保有しており、
前記記録媒体は、ソフトウェアを格納しており、
前記実行器は、自己の外部からは情報の読み出しおよび書き込みが困難な記憶領域に、乱数を格納しており、
実行許可情報の配布を求める際、前記実行器は、前記ソフト配布器に対して、格納している乱数を通知し、
前記ソフト配布器は、通知された乱数で実行許可情報を暗号化して、前記実行器へ配布し、
前記実行器は、暗号化された実行許可情報の配布を受けると、
配布された暗号化された実行許可情報を、格納している乱数で復号し、
復号に連携して、格納している乱数を更新することを特徴とする、ソフトウェア実行制御システム。
【請求項１８】　ソフトウェアを実行する実行器と、当該実行器に情報伝達可能に接続され、かつ情報の読み出しおよび書き込みが可能な記録媒体と、実行器の求めに応じて、実行許可情報を配布するソフト配布器とからなり、実行器が保有している実行許可情報に、ソフト配布器から追加で配布される実行許可情報を加え、かつ実行許可情報の不正な使用を防止するためのソフトウェア実行制御システムであって、
前記実行器は、自己の外部からは情報の読み出しおよび書き込みが困難な記憶領域に、第１および第２の乱数を格納しており、
前記記録媒体は、ソフトウェアおよび第１の暗号化された実行許可情報を格納しており、
前記ソフト配布器は、第２の実行許可情報を保有しており、
前記実行器は、前記第２の実行許可情報の配布を求める際に、前記ソフト配布器に対して前記第２の乱数を通知し、
前記ソフト配布器は、通知された第２の乱数で前記第２の実行許可情報を暗号化して、前記実行器に配布し、
前記実行器は、第２の暗号化された実行許可情報を受け取ると、
受け取った第２の暗号化された実行許可情報を、格納している第２の乱数で復号して、第２の実行許可情報を求め、
第２の暗号化された実行許可情報の復号に連携して、格納している第２の乱数を更新し、
前記記録媒体から第１の暗号化された実行許可情報を獲得して、格納している第１の乱数で復号して、第１の実行許可情報を求め、
第１の暗号化された実行許可情報の復号に連携して、格納している第１の乱数を更新し、
求めた第１および第２の実行許可情報に基づいて、第３

の実行許可情報を作成し、
作成した第３の実行許可情報を、更新した第１の乱数で暗号化して、前記記録媒体に格納することを特徴とする、ソフトウェア実行制御システム。
【請求項１９】　ソフトウェアを実行する第１および第２の実行器と、情報の読み出しおよび書き込みが可能な記録媒体とからなり、第１の実行器が保有している実行許可情報を第２の実行器へ譲渡し、かつ実行許可情報の不正な使用を防止するためのソフトウェア実行制御システムであって、
前記第１の実行器は、自己の外部からは情報の読み出しおよび書き込みが困難な記憶領域に、乱数を格納しており、
前記記録媒体は、ソフトウェアおよび暗号化された実行許可情報を格納しており、
前記第１の実行器から前記第２の実行器に対して、前記第１の実行器が保有している実行許可情報を譲渡する際に、前記第１の実行器と前記第２の実行器とを情報伝達可能に接続し、
前記第１の実行器は、
自己の格納している乱数を前記第２の実行器に通知し、
通知に連携して、自己の格納している乱数を更新し、
前記第２の実行器は、乱数の通知を受けると、通知された乱数を、自己の外部からは情報の読み出しおよび書き込みが困難な記憶領域に格納することを特徴とする、ソフトウェア実行制御システム。
【請求項２０】　ソフトウェアを実行する第１および第２の実行器と、それぞれの実行器に情報伝達可能に接続され、かつ情報の読み出しおよび書き込みが可能な第１および第２の記録媒体とからなり、前記第１の実行器が保有している実行許可情報の一部を前記第２の実行器に譲渡し、かつ、実行許可情報の不正な使用を防止するためのソフトウェア実行制御システムであって、
前記第１の実行器は、自己の外部からは情報の読み出しおよび書き込みが困難な記憶領域に、第１および第２の乱数を格納しており、
前記第１の記録媒体は、ソフトウェアおよび暗号化された実行許可情報を格納しており、
前記第２の記録媒体は、ソフトウェアを格納しており、
前記第１の実行器から前記第２の実行器に対して、前記第１の実行器が保有している実行許可情報の一部を譲渡する際に、前記第１の実行器と前記第２の実行器とを情報伝達可能に接続し、
前記第１の実行器は、
前記第１の記録媒体から暗号化された実行許可情報を獲得して、格納している第１の乱数で復号し、
復号に連携して、格納している第１の乱数を更新し、
復号して求めた実行許可情報を、第１の実行許可情報と第２の実行許可情報とに分割し、
分割して得た第１の実行許可情報を、更新した第１の乱数で暗号化して、前記第１の記録媒体に格納し、
分割して得た第２の実行許可情報を、格納している第２の乱数で暗号化し、
前記第２の乱数と、第２の暗号化された実行許可情報とを、前記第２の実行器に通知し、
通知に連携して、格納している第２の乱数を更新し、
前記第２の実行器は、第２の乱数と第２の暗号化された実行許可情報とを受け取ると、前記第２の乱数を自己の外部からは情報の読み出しおよび書き込みが困難な記憶領域に、第２の暗号化された実行許可情報を第２の記録媒体に、それぞれ格納することを特徴とする、ソフトウェア実行制御システム。
【請求項２１】　ソフトウェアを実行するにはソフト鍵を必要とし、かつソフト鍵の不正な使用を防止するためのソフトウェア実行制御システムであって、
暗号化されたソフトウェアおよび暗号化されたソフト鍵を格納し、かつ情報の読み出しおよび書き込みが可能な記録媒体が、ソフトウェアを実行する実行器に情報伝達可能に接続され、
前記実行器は、
乱数を格納し、かつ自己の外部からは情報の読み出しおよび書き込みが困難な乱数格納手段と、
前記記録媒体から暗号化されたソフト鍵を獲得して、前記乱数格納手段から取得した乱数で復号する第１の復号手段と、
前記記録媒体から暗号化されたソフトウェアを獲得して、前記第１の復号手段の復号によって得られたソフト鍵で復号する第２の復号手段と、
前記第２の復号手段の復号によって得られたソフトウェアを実行するソフト実行手段と、
ソフトウェアの実行に関連して、前記乱数格納手段に格納された乱数を更新する乱数更新手段と、
前記第１の復号手段の復号によって得られたソフト鍵を、更新された乱数で暗号化して、前記記録媒体に格納する暗号化手段とを備える、ソフトウェア実行制御システム。
【請求項２２】　実行回数が所定の条件を満足する場合に、ソフトウェアを実行し、かつ当該実行回数の不正な使用を防止するためのソフトウェア実行制御システムであって、
ソフトウェアおよび暗号化された実行回数を格納し、かつ情報の読み出しおよび書き込みが可能な記録媒体が、ソフトウェアを実行する実行器に情報伝達可能に接続され、
前記実行器は、
乱数を格納し、かつ自己の外部からは情報の読み出しおよび書き込みが困難な乱数格納手段と、
前記記録媒体から暗号化された実行回数を獲得して、前記乱数格納手段から取得した乱数で復号する復号手段と、

前記復号手段の復号によって得られた実行回数が、所定の条件を満足するか否かを検査し、所定の条件を満足する場合に、ソフトウェアの実行を指示する実行回数検査手段と、
前記実行回数検査手段からの指示に応答して、ソフトウェアを実行するソフト実行手段と、
ソフトウェアの実行にともなって、復号によって得られた実行回数を更新する実行回数更新手段と、
ソフトウェアの実行に連携して、前記乱数格納手段に格納された乱数を更新する乱数更新手段と、
更新された実行回数情報を、更新された乱数で暗号化して、前記記録媒体に格納する暗号化手段とを備える、ソフトウェア実行制御システム。

【請求項２３】　実行回数が所定の条件を満足する場合に、ソフト鍵で復号して得られたソフトウェアを実行し、かつ実行回数およびソフト鍵の不正な使用を防止するためのソフトウェア実行制御システムであって、
暗号化されたソフトウェアおよび暗号化されたソフト鍵／実行回数を格納し、かつ情報の読み出しおよび書き込みが可能な記録媒体が、ソフトウェアを実行する実行器に情報伝達可能に接続され、
前記実行器は、
乱数を格納し、かつ自己の外部からは情報の読み出しおよび書き込みが困難な乱数格納手段と、
前記記録媒体から暗号化されたソフト鍵／実行回数を獲得して、前記乱数格納手段から取得した乱数で復号する第１の復号手段と、
前記記録媒体から暗号化されたソフトウェアを獲得して、前記第１の復号手段の復号によって得られたソフト鍵で復号する第２の復号手段と、
前記第１の復号手段の復号によって得られた実行回数が、所定の条件を満足するか否かを検査し、所定の条件を満足する場合に、ソフトウェアの実行を指示する実行回数検査手段と、
前記実行回数検査手段からの指示に応答して、前記第２の復号手段の復号によって得られたソフトウェアを実行するソフト実行手段と、
ソフトウェアの実行に伴って、復号によって得られた実行回数を更新する実行回数更新手段と、
ソフトウェアの実行に連携して、前記乱数格納手段に格納された乱数を更新する乱数更新手段と、
復号によって得られたソフト鍵と更新された実行回数とを、更新された乱数で暗号化して前記記録媒体に格納する暗号化手段とを備える、ソフトウェア実行制御システム。

【請求項２４】　実行回数が所定の条件を満足する場合に、ソフト鍵で復号して得られたソフトウェアを実行し、かつソフト鍵および実行回数の不正な使用を防止するためのソフトウェア実行制御システムであって、
複数の、暗号化されたソフトウェア、暗号化されたソフト鍵／実行回数および暗号化された補助鍵が格納され、かつ情報の読み出しおよび書き込みが可能な記録媒体が、ソフトウェアを実行する実行器に情報伝達可能に接続され、
前記実行器は、
乱数を格納し、かつ自己の外部からは情報の読み出しおよび書き込みが困難な乱数格納手段と、
前記記録媒体から、当該ソフトウェアに専用の暗号化された補助鍵を獲得して、前記乱数格納手段から取得した乱数で復号する第１の復号手段と、
前記記録媒体から、当該ソフトウェアに専用の暗号化されたソフト鍵／実行回数を獲得して、前記第１の復号手段の復号によって得られた補助鍵で復号する第２の復号手段と、
前記記録媒体から暗号化されたソフトウェアを獲得して、前記第２の復号手段の復号によって得られたソフト鍵で復号する第３の復号手段と、
前記第２の復号手段の復号によって得られた実行回数が、所定の条件を満足するか否かを検査し、所定の条件を満足する場合に、当該ソフトウェアの実行を指示する実行回数検査手段と、
前記実行回数検査手段からの指示に応答して、前記第３の復号手段の復号によって得られたソフトウェアを実行するソフト実行手段とソフトウェアの実行に伴って、前記第２の復号手段の復号によって得られた実行回数を更新する実行回数更新手段と、
前記第２の復号手段の復号によって得られたソフト鍵と、前記実行回数更新手段によって更新された実行回数とを、前記第１の復号手段の復号によって得られた補助鍵で暗号化して、前記記録媒体に格納する第１の暗号化手段と、
所定のタイミングで、前記記録媒体から全ての暗号化された補助鍵を獲得して、前記乱数格納手段から取得した乱数で復号する第４の復号手段と、
前記第４の復号手段の復号に連携して、前記乱数格納手段に格納された乱数を更新する乱数更新手段と、
前記第４の復号手段の復号によって得られた補助鍵を、前記乱数更新手段によって更新された乱数で暗号化して、前記記録媒体に格納する第２の暗号化手段とを備える、ソフトウェア実行制御システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ソフトウェア実行制御システムに関し、より特定的には、ソフトウェアの不正使用を防止するためのソフトウェア実行制御システムに関する。

【０００２】

【従来の技術】近年、種々のマルチメディア機器が開発され、ゲームや教育用のソフトウェアをはじめとする多くの有償マルチメディアソフトウェアが販売されてい

る。ところが、それらのソフトウェアの保護は不完全であり、不正コピーのソフトウェアが数多く出回っているのが現状である。ソフトウェアの不正使用を防ぐために、特許法や著作権法等の、法律による規制があるが、同時に、不正にコピーされたソフトウェアを実行できないようにする実行制御システムが開発されている。

【０００３】例えば、特開昭６１－１４５６４２号公報に、ソフトウェアの実行に必要なソフト鍵を実行器に固有の情報で暗号化することにより、ソフトウェアの不正使用を防止する方法が提案されている。ここで開示されている構成の一部を変更して第１の従来例とする。さらに、この第１の従来例において、実行回数を制限されたソフトウェアの不正使用を防止する方法を第２の従来例とする。また、例えば、特公平３－３２８１３号公報に、ソフトウェアの実行を制御するためのコプロッセサを実行器に接続する方法が提示されている。この方法を、実行回数を制限するよう構成の一部を変更して第３の従来例とする。

【０００４】（第１の従来例）図９は、第１の従来例に係るソフトウェア実行制御システムの構成を示すブロック図である。図９において、実行器１０１は、あるソフトウェアＳｏｆｔＡを実行することを許可された、特定の実行器である。実行器１０１は、自己に固有の秘密情報Ｓｘ（固有鍵）を格納するための固有鍵格納部１０２を内蔵する。固有鍵格納部１０２は、実行器１０１の外部からは、読み出しおよび書き込みができないものとする。図では、こうした領域はハッチングをかけて表されている。記録媒体１０３は、実行器１０１で実行するソフトウェアを格納するための記録媒体である。鍵Ｋによりデータ Ｄを暗号化することをＥ（Ｋ，Ｄ）と表すことにすると、記録媒体１０３には、ソフト鍵Ｋで暗号化された暗号化ソフトＥ（Ｋ，ＳｏｆｔＡ）、および実行器１０１の固有鍵Ｓｘで暗号化された暗号化ソフト鍵Ｅ（Ｓｘ，Ｋ）が格納されている。ソフトウェアＳｏｆｔＡを実行する際には、実行器１０１は、最初、記録媒体１０３から暗号化ソフト鍵Ｅ（Ｓｘ，Ｋ）を得て、得た暗号化ソフト鍵Ｅ（Ｓｘ，Ｋ）を、復号部１０４において、固有鍵格納部１０２から獲得した固有鍵Ｓｘで復号してソフト鍵Ｋを求める。次に、実行器１０１は、記録媒体１０３から暗号化ソフトＥ（Ｋ，ＳｏｆｔＡ）を得て、復号部１０５において、求めたソフト鍵Ｋで復号してソフトウェアＳｏｆｔＡを求め、これを実行する。

【０００５】本従来例では、記録媒体に格納されている暗号化ソフトＥ（Ｋ，ＳｏｆｔＡ）および暗号化ソフト鍵Ｅ（Ｓｘ，Ｋ）をコピーしても、固有鍵Ｓｘを保有している実行器以外では暗号化ソフト鍵Ｅ（Ｓｘ，Ｋ）を復号できないため、ソフトウェアの実行はできない。また、固有鍵Ｓｘが格納されている固有鍵格納部１０２は、実行器１０１による以外は読み出しおよび書き込みができない領域なので、固有鍵Ｓｘの複製はできない。これにより、不正にコピーされたソフトウェアの実行を防止している。

【０００６】ところで、本従来例は、初めに一度料金を支払って実行器１０１用の暗号化ソフト鍵を入手すれば、実行器１０１は、そのソフトウェアを何度でも実行できる場合を想定している。ソフトウェアの購入形態としては、このいわゆる「買取り制」以外に、ソフトウェアの使用量に応じて料金を支払う「従量制」の形態がある。さらに、この「従量制」を実現する方法は大きく分けて２つあって、その第１は、ソフトウェアを実行する回数や有効期限などの条件を予めソフト販売者とユーザとの間で契約し、その範囲で実行を許可する「実行制御方法」であり、第２は、実行器におけるソフトウェアの実行履歴に関する情報を蓄積し、後日、それに応じた料金を支払う方法である。

【０００７】本従来例の不正防止方法は、上記のような「従量制」の形態のソフトウェアに対応する機能を備えていない。そこで、「従量制」の形態のソフトウェアについても不正使用を防止できるようにした方法が、以下に説明する第２の従来例である。ただし、第２の従来例は、上記の２つの方法のうち、「実行制御方法」を採用しており、簡単のために、ソフトウェアを実行する回数を制限する場合に限定している。なお、後に説明する第３の従来例ならびに第１および第２の実施形態においても同様に、ソフトウェアの実行に関する制限を、実行回数の制限に限定している。また、ソフト販売者とユーザとの間で契約し、ユーザが得る情報を「実行許可情報」と呼ぶことにし、ユーザは、この実行許可情報の範囲内で、ソフトウェアを実行することができるものとする。従って、以下では、「実行許可情報」とは、ソフトウェアを所定の回数実行する権利を意味する。

【０００８】（第２の従来例）図１０は、第２の従来例に係るソフトウェア実行制御システムの構成を示すブロック図である。図１０において、ソフト鍵Ｋおよび実行回数ｎを実行器１０１の固有鍵Ｓｘで暗号化した暗号化ソフト鍵／実行回数Ｅ（Ｓｘ，（Ｋ，ｎ））が、暗号化ソフトＥ（Ｋ，ＳｏｆｔＡ）と共に記録媒体１０３に格納されている。ここで、実行回数とは、残りの実行可能な回数を意味する（以下においても同様である）。ソフトウェアＳｏｆｔＡを実行する際には、実行器１０１は、最初、記録媒体１０３から暗号化ソフト鍵／実行回数Ｅ（Ｓｘ，（Ｋ，ｎ））を獲得し、これを復号部１０４において固有鍵Ｓｘで復号して、ソフト鍵Ｋおよび実行回数ｎを求める。次に、実行器１０１は、復号部１０５において、ソフト鍵Ｋにより暗号化ソフトＥ（Ｋ，ＳｏｆｔＡ）を復号して、ソフトウェアＳｏｆｔＡを求める一方、実行回数検査部１０６において、実行回数ｎが１以上であるか否かを検査する。ｎが１以上であれば、実行器１０１は、復号したソフトウェアＳｏｆｔＡを実行する。ソフトウェアＳｏｆｔＡの実行後、実行器１０

1は、実行回数更新部107において実行回数nを1減少してn′（＝n－1）に更新し、続いて、暗号部108において、このn′をソフト鍵Kと共に固有鍵Sxで暗号化する。そして、実行器101は、この更新された暗号化ソフト鍵／実行回数E（Sx，（K，n′））を記録媒体103に再び格納する。

【0009】（第3の従来例）図11は、第3の従来例に係るソフトウェア実行制御システムの構成を示すブロック図である。図11において、このソフトウェア実行システムは、読み出し専用の記録媒体110と、ソフトウェアを実行する実行器111と、実行器111に接続されてソフトウェアの実行制御を行い、かつ、外部からは情報の読み出しおよび書き込みの困難なコプロセッサ112とを備えている。コプロセッサ112に含まれる固有鍵格納部113に、実行器111に固有の鍵Syが格納されており、記録媒体110には、第2の従来例と同様に、ソフト鍵Kで暗号化された暗号化ソフトE（K，SoftA）と、固有鍵Syで暗号化された暗号化ソフト鍵／実行回数E（Sy，（K，n））とが格納されている。

【0010】本従来例では、最初、ユーザは、記録媒体110に格納された情報を、コプロセッサ112にインストールする。コプロセサ112は、インストールされた暗号化ソフト鍵／実行回数E（Sy，（K，n））を、復号部114において固有鍵Syで復号し、ソフト鍵Kおよび実行回数nを求め、求めたソフト鍵Kおよび実行回数nを、自己の内部のソフト鍵格納部115および実行回数格納部116にそれぞれ格納する。次に、コプロセサ112は、インストールされた暗号化ソフトE（K，SoftA）を、復号部117において求めたソフト鍵Kで復号し、実行回数検査部119において、実行回数nが1以上であることを検査する。実行回数nが1以上であれば、実行器111は、ソフトウェアSoftAを実行する。この際、コプロセッサ112は、実行回数更新部118において、実行回数nを1減少してn′とし、このn′を実行回数格納部116に格納する。なお、このインストールにより、記録媒体110の暗号化ソフト鍵／実行回数E（Sy，（K，n））に関する部分は無効化され、再びインストールすることはできない。

【0011】

【発明が解決しようとする課題】上記第1の従来例に、実行回数を制限する機能を加えた上記第2の従来例では、以下に述べる二つの問題がある。その第一は、ユーザが、実行回数nが0になる以前の記録媒体をコピーしておけば、コピーのソフトウェアを、コピーした時点での実行回数分だけ実行することができるという問題である。コピーのコピーを実行することも可能であり、従って、実質的にソフトウェアは無限回実行可能となる（以下ではこれを第1の攻撃と呼ぶことにする）。

【0012】その第二は、実行の度に実行回数nを1ずつ減少してn′とし、これに伴って更新した暗号化ソフト鍵／実行回数E（Sx，（K，n′））を記録媒体に書き込むが、この書き込みを妨害することにより、実行回数の制限を実質的に無効にすることができるという問題である。すなわち、記録媒体に格納されている実行許可情報に含まれる実行回数nは、実行しても減少しない（以下ではこれを第2の攻撃と呼ぶことにする）。

【0013】上記第1および第2の攻撃を防ぐため、上記第3の従来例では、第2の従来例の実行制御に関わる構成要素を、外部からは読み出しおよび書き込みができないコプロセッサ内に設けるようにしている。ところが、こうした専用のコプロセッサを備えるとコストが高くなるという問題がある。しかも、第2の従来例では、ソフト鍵および実行回数を格納する場所は、ソフトウェアを格納している記録媒体であるのに対し、第3の従来例では、第2の従来例の構成要素に加えて、ソフト鍵および実行回数を格納するための記憶領域を、コプロセッサ内に、さらに備えることが必要である。特に、複数のソフトウェアを同時に扱う場合には、それぞれのソフトウェアについて、こうした記憶領域を確保しなければならないため、よりコスト高となる問題がある。

【0014】したがって、本発明の目的は、実行回数を制限されたソフトウェアに対する上記第1および第2の攻撃を防止することである。さらに、本発明の他の目的は、実行回数を制限されたソフトウェアを、同時に複数取り扱う場合にも、上記第1および第2の攻撃を防止すると同時に、備える必要のある読み出しおよび書き込みが困難な記憶領域を、できるだけ小さくすることである。

【0015】

【課題を解決するための手段および発明の効果】以下には、上記目的を達成するための本発明の構成を示すが、後述する実施形態との対応関係を明確にするために、本発明で採用される各構成要素には、対応する部分の参照番号を付しておく。ただし、この参照番号は、あくまでも理解を容易にするためおよび参考のために付されるのであって、本発明の請求の範囲を限定的に解釈するものではないことを予め指摘しておく。

【0016】第1の発明は、予め定められた実行許可情報に従ってソフトウェアの実行を制御し、かつ当該実行許可情報の不正な使用を防止するためのソフトウェア実行制御システムであって、ソフトウェアおよび暗号化された実行許可情報を格納し、かつ情報の読み出しおよび書き込みが可能な記録媒体（1）が、ソフトウェアを実行する実行器（2）に情報伝達可能に接続され、実行器（2）は、乱数を格納し、かつ自己の外部からは情報の読み出しおよび書き込みが困難な乱数格納手段（3）と、記録媒体（1）から暗号化された実行許可情報を獲得して、乱数格納手段（3）から取得した乱数で復号す

る復号手段（4）と、記録媒体（1）からソフトウェアを獲得して、復号手段（4）の復号によって得られた実行許可情報に従って実行するソフト実行手段（7）と、ソフトウェアの実行に関連して、乱数格納手段（3）に格納された乱数を更新する乱数更新手段（9）と、復号手段（4）の復号によって得られた実行許可情報を、ソフト実行手段（7）がソフトウェアを実行した後に、乱数更新手段（9）によって更新された乱数で暗号化して、記録媒体（1）に格納する暗号化手段（10）とを備えている。

【0017】上記のように、第1の発明は、ソフトウェアを実行する実行器と、ソフトウェアおよび暗号化された実行許可情報を格納している記録媒体とで構成されている。最初、実行器に備えられた復号手段は、記録媒体から暗号化された実行許可情報を獲得し、乱数格納手段に格納された乱数で復号して実行許可情報を求める。次に、ソフト実行手段は、求められた実行許可情報に従ってソフトウェアを実行する。ソフトウェアの実行に関連して、乱数更新手段は乱数格納手段に格納された乱数を更新する。次に、暗号化手段は、更新された実行許可情報を、更新された乱数で暗号化して記録媒体に格納する。

【0018】このように、実行器の内部の、情報の読み出しおよび書き込みが困難な乱数格納手段に乱数を格納しておき、この乱数で実行許可情報を暗号化する。ソフトウェアの実行に関連して、乱数を更新することにより、正規の実行器以外の実行器でソフトウェアが不正に実行されるのを防止することができる。また、第1の発明では、読み出しおよび書き込みが困難な乱数格納手段は、1個の乱数を格納するだけの大きさの領域を準備すればよく、実現するためのコストも最小にすることができる。

【0019】第2の発明は、第1の発明において、ソフトウェアの実行にともなって、復号手段（4）の復号によって得られた実行許可情報を更新する実行許可情報更新手段（8）をさらに備え、暗号化手段（10）は、実行許可情報更新手段（8）によって更新された実行許可情報を、乱数更新手段（9）によって更新された乱数で暗号化して、記録媒体（2）に格納することを特徴としている。

【0020】上記のように、第2の発明は、第1の発明において、実行許可情報更新手段をさらに備えている。実行許可情報更新手段は、ソフトウェアの実行にともなって実行許可情報を更新し、暗号化手段は、実行許可情報更新手段によって更新された実行許可情報を暗号化して記録媒体に格納する。これにより、第2の発明は、コピーされた実行許可情報の不正使用を防止することができる。すなわち、記録媒体に格納された、暗号化された実行許可情報をある時点でコピーして保存しておき、1回以上ソフトウェアを実行した後に、記録媒体に格納されている暗号化された実行許可情報を、このコピーされた暗号化された実行許可情報に差し替える。このとき、実行器の保有する乱数は実行に関連して更新されているため、実行器は、このコピーされた暗号化された実行許可情報を復号することができない。また、第2の発明は、更新された実行許可情報の記録媒体への書き込みを妨害して、更新を事実上無効にする攻撃を防止することができる。すなわち、実行器は、ソフトウェアの実行の際、自己の保有する乱数を更新しているため、更新前の暗号化された実行許可情報を、もはや復号することができない。

【0021】第3の発明は、第1または第2の発明において、乱数更新手段（9）が、ソフトウェアの実行毎に、乱数格納手段（3）に格納された乱数を更新することを特徴としている。

【0022】このように、第3の発明では、ソフト実行手段がソフトウェアを実行するごとに、乱数更新手段は乱数格納手段に格納された乱数を更新する。これにより、ソフトウェアの不正な使用の防止効果を最も大きくすることができる。

【0023】第4の発明は、第1または第2の発明において、乱数更新手段（9）が、予め決められた複数回のソフトウェアの実行に一度、乱数格納手段（3）に格納された乱数を更新することを特徴としている。

【0024】このように、第4の発明では、ソフト実行手段がソフトウェアを予め決められた複数回実行するごとに一度、乱数更新手段は乱数格納手段に格納された乱数を更新する。これにより、実行制御に要する処理の負荷を軽減しながら、ソフトウェアの不正使用を効果的に防止することができる。

【0025】第5の発明は、第1または第2の発明において、乱数更新手段（9）が、予め決められた可変の回数のソフトウェアの実行に一度、乱数格納手段（3）に格納された乱数を更新し、乱数の更新の間隔に関する情報を、ソフトウェア使用者に秘密にすることを特徴としている。

【0026】このように、第5の発明では、ソフト実行手段がソフトウェアを予め決められた可変の回数実行するごとに一度、乱数更新手段は乱数格納手段に格納された乱数を更新する。これにより、乱数の更新の頻度に対する不正防止の効果を高めることができる。

【0027】第6の発明は、第1または第2の発明において、乱数格納手段（3）は、実行器（2）に設けられる代わりに、記録媒体（1）に設けられることを特徴としている。

【0028】上記のように、第6の発明では、記録媒体が乱数格納手段を備え、実行器は、ソフトウェアを実行する際に、この乱数格納手段に格納された乱数を取得する。実行器は、取得した乱数で暗号化された実行許可情報を復号して実行許可情報を求め、求めた実行許可情報

に従ってソフトウェアを実行する。次に、実行器は、乱数を更新し、更新した乱数を記録媒体内の乱数格納手段に格納する。このように、記録媒体に格納された暗号化された実行許可情報を、当該記録媒体に格納された乱数で復号するため、ソフトウェアを実行する実行器を特定することなく、実行制御を行うことができる。

【００２９】第７の発明は、第１または第２の発明において、記録媒体（１）の代わりに、読み出し専用の第１の記録媒体と、読み出しおよび書き込みが可能な第２の記録媒体とが実行器（２）に接続され、第１の記録媒体はソフトウェアを格納し、第２の記録媒体は暗号化された実行許可情報を格納することを特徴としている。

【００３０】このように、第７の発明では、読み出し専用の記録媒体にソフトウェアを格納し、読み出しおよび書き込みが可能な記録媒体には暗号化された実行許可情報を格納する。これにより、乱数の更新にともなって書き換えが必要な実行許可情報は、読み出しおよび書き込みが可能な記録媒体に格納するが、更新の必要がないソフトウェアの格納には、読み出し専用の記録媒体を用いることができる。

【００３１】第８の発明は、第１または第２の発明において、記録媒体（１）に格納されたソフトウェアは、暗号化されており、ソフト実行手段（７）は、記録媒体（１）から暗号化されたソフトウェアを獲得して、復号手段（４）の復号によって得られた実行許可情報に従って復号し、復号して得たソフトウェアを実行することを特徴としている。

【００３２】上記のように、第８の発明では、記録媒体に格納されたソフトウェアは暗号化されており、ソフト実行手段は、復号手段の復号によって得られた実行許可情報に従って、暗号化されたソフトウェアを復号し、復号して得たソフトウェアを実行する。このように、ソフトウェアを暗号化しておくことにより、さらに安全性を高めることができる。

【００３３】第９の発明は、予め定められた実行許可情報に従ってソフトウェアの実行を制御し、かつ当該実行許可情報の不正な使用を防止するためのソフトウェア実行制御システムであって、複数の、ソフトウェア、暗号化された実行許可情報および暗号化された補助鍵を格納し、かつ情報の読み出しおよび書き込みが可能な記録媒体（２０）が、ソフトウェアを実行する実行器（２１）に情報伝達可能に接続され、実行器（２１）は、乱数を格納し、かつ自己の外部からは情報の読み出しおよび書き込みが困難な乱数格納手段（２２）と、記録媒体（２０）から暗号化された補助鍵を獲得して、乱数格納手段（２２）から取得した乱数で復号する第１の復号手段（２３）と、記録媒体（２０）から暗号化された実行許可情報を獲得して、第１の復号手段（２３）の復号によって得られた補助鍵で復号する第２の復号手段（２４）と、記録媒体（２０）から対応するソフトウェアを獲得して、第２の復号手段（２４）の復号によって得られた実行許可情報に従って実行するソフト実行手段（２９）と、第２の復号手段（２４）の復号によって得られた実行許可情報を、ソフト実行手段（２９）が対応するソフトウェアを実行した後に、第１の復号手段（２３）の復号によって得られた補助鍵で暗号化して、記録媒体（２０）に格納する第１の暗号化手段（２８）と、ソフトウェアの実行に関連して、記録媒体（２０）から全ての暗号化された補助鍵を獲得して、乱数格納手段（２２）に格納された乱数で復号する第３の復号手段（３０）と、第３の復号手段（３０）の復号に連携して、乱数格納手段（２２）に格納された乱数を更新する乱数更新手段（３１）と、第３の復号手段（３０）の復号によって得られた補助鍵を、乱数更新手段（３１）によって更新された乱数で暗号化して、記録媒体（２０）に格納する第２の暗号化手段（３２）とを備えている。

【００３４】上記のように、第９の発明は、ソフトウェアを実行する実行器と、複数の、ソフトウェア、暗号化された実行許可情報および暗号化された補助鍵が格納された記録媒体とで構成される。最初、実行器に備えられた第１の復号手段は、記録媒体から、実行すべきソフトウェアに対応する暗号化された補助鍵を獲得し、乱数格納手段に格納された乱数で復号して補助鍵を求める。次に、第２の復号手段は、記録媒体から当該ソフトウェアに対応する暗号化された実行許可情報を獲得し、第１の復号手段の復号によって求められた補助鍵で復号して、実行許可情報を得る。ソフト実行手段は、得られた実行許可情報に従って、当該ソフトウェアを実行する。続いて、第１の暗号化手段は、第１の復号手段の復号によって求められた補助鍵で、得られた実行許可情報を暗号化して記録媒体に格納する。また、第３の復号手段は、ソフトウェアの実行に関連して、記録媒体から、全ての暗号化された補助鍵を獲得し、乱数格納手段に格納された乱数で復号して補助鍵を求める。第３の復号手段の復号に連携して、乱数更新手段は乱数格納手段に格納された乱数を更新する。第２の暗号化手段は、第３の復号手段の復号によって求められた補助鍵を、更新された乱数で暗号化して記録媒体に格納する。

【００３５】このように、一つの実行器で複数のソフトウェアを取り扱う場合には、ソフトウェア毎の実行許可情報をそれぞれに専用の補助鍵で暗号化し、さらに、これらの補助鍵を乱数で暗号化する。そして、ソフトウェアの実行に関連して乱数を更新することにより、第１の発明と同様に、正規の実行器以外の実行器でソフトウェアが不正に実行されるのを防止することができる。また、取り扱うソフトウェアの数に関わらず、使用する乱数は一つだけでよため、乱数を格納するための読み出しおよび書き込みが困難な記憶領域は、一つの乱数を格納するだけの大きさを備えればよい。

【００３６】第１０の発明は、第９の発明において、ソ

フトウェアの実行にともなって、第2の復号手段（24）の復号によって得られた実行許可情報を更新する実行許可情報更新手段（27）をさらに備え、第1の暗号化手段（28）は、実行許可情報更新手段（27）によって更新された実行許可情報を、第1の復号手段（23）の復号によって得られた補助鍵で暗号化して、記録媒体（20）に格納することを特徴としている。

【0037】上記のように、第10の発明では、実行許可情報更新手段が、ソフトウェアの実行にともなって実行許可情報を更新し、第1の暗号化手段は、実行許可情報更新手段によって更新された実行許可情報を補助鍵で暗号化する。これにより、第10の発明は、一つの実行器で複数のソフトウェアを取り扱う場合にも、第2の発明と同様にして、コピーされた実行許可情報の不正な使用、および更新された実行許可情報の記録媒体への書き込み妨害を防止することができる。

【0038】第11の発明は、第9または第10の発明において、第3の復号手段（30）が、ソフトウェアの実行毎に記録媒体（20）から全ての暗号化された補助鍵を獲得して、乱数格納手段（22）に格納された乱数で復号することを特徴としている。

【0039】このように、第11の発明では、ソフト実行手段がソフトウェアを実行するごとに、第3の復号手段は記録媒体から暗号化された補助鍵を獲得して、乱数新手段に格納された乱数で復号する。これにより、ソフトウェアの不正な使用の防止効果を最も大きくすることができる。

【0040】第12の発明は、第9または第10の発明において、第3の復号手段（30）が、予め決められた複数回のソフトウェアの実行に一度、記録媒体（20）から全ての暗号化された補助鍵を獲得して、乱数格納手段（22）に格納された乱数で復号することを特徴としている。

【0041】上記のように、第12の発明では、ソフト実行手段がソフトウェアを予め決められた複数回実行するごとに一度、第3の復号手段は記録媒体から全ての暗号化された補助鍵を獲得して、乱数格納手段に格納された乱数で復号する。これにより、実行制御に要する処理の負荷を軽減しながら、ソフトウェアの不正な使用を効果的に防止することができる。

【0042】第13の発明は、第9または第10の発明において、第3の復号手段（30）は、予め決められた可変の回数のソフトウェアの実行に一度、記録媒体（20）から全ての暗号化された補助鍵を獲得して、乱数格納手段（22）に格納された乱数で復号し、暗号化された補助鍵の復号の間隔に関する情報をソフトウェア使用者に秘密にすることを特徴としている。

【0043】上記のように、第13の発明では、ソフト実行手段がソフトウェアを予め決められた可変の数回実行するごとに一度、第3の復号手段は記録媒体から全ての暗号化された補助鍵を獲得して、乱数格納手段に格納された乱数で復号する。また、補助鍵の復号に関する情報は、ソフトウェア使用者に秘密にされる。これにより、乱数の更新の頻度に対する不正防止の効果を高めることができる。

【0044】第14の発明は、第9または第10の発明において、乱数格納手段（22）は、実行器（21）に設けられる代わりに、記録媒体（20）に設けられることを特徴としている。

【0045】このように、第14の発明では、記録媒体が乱数格納手段を備え、実行器は、ソフトウェアを実行する際に、記録媒体から乱数を取得する。実行器は、取得した乱数で、暗号化された実行許可情報を復号して実行許可情報を求め、求めた実行許可情報に従ってソフトウェアを実行する。実行器は、ソフトウェアの実行に連携して乱数を更新し、実行後に、更新した乱数を記録媒体内の乱数格納手段に格納する。このように、記録媒体に格納された暗号化された実行許可情報を当該記録媒体に格納された乱数で復号するため、ソフトウェアを実行する実行器を特定することなく、実行制御を行うことができる。

【0046】第15の発明は、第9または第10の発明において、記録媒体（20）の代わりに、読み出し専用の第1の記録媒体と、読み出しおよび書き込みが可能な第2の記録媒体とが実行器に接続され、第1の記録媒体はソフトウェアを格納し、第2の記録媒体は暗号化された実行許可情報を格納し、乱数格納手段（22）は、実行器（21）に設けられる代わりに、第2の記録媒体に設けられることを特徴としている。

【0047】このように、第15の発明では、読み出し専用の記録媒体にソフトウェアを格納し、読み出しおよび書き込みが可能な記録媒体には暗号化された実行許可情報を格納する。これにより、乱数の更新にともなって書き換えが必要な実行許可情報は、読み出しおよび書き込みが可能な記録媒体に格納するが、更新の必要がないソフトウェアの格納には、読み出し専用の記録媒体を用いることができる。また、第2の記録媒体に乱数格納手段を設けることにより、第2の記録媒体に格納された暗号化された実行許可情報を当該記録媒体に格納された乱数で復号することになり、ソフトウェアを実行する実行器を特定することなく、実行制御を行うことができる。

【0048】第16の発明は、第9または第10の発明において、記録媒体（20）に格納されたソフトウェアは、それぞれ暗号化されており、ソフト実行手段（29）は、記録媒体（20）から、対応する暗号化されたソフトウェアを獲得して、第2の復号手段（24）の復号によって得られた実行許可情報に従って復号し、復号して得たソフトウェアを実行することを特徴としている。

【0049】上記のように、第16の発明では、記録媒

体に格納されたソフトウェアはそれぞれ暗号化されており、ソフト実行手段は、第2の復号手段の復号によって得られた実行許可情報に従って、対応する暗号化されたソフトウェアを復号し、復号して得たソフトウェアを実行する。このように、ソフトウェアをそれぞれ暗号化しておくことにより、さらに安全性を高めることができる。

【0050】第17の発明は、ソフトウェアを実行する実行器（2または21）と、当該実行器（2または21）に情報伝達可能に接続され、かつ情報の読み出しおよび書き込みが可能な記録媒体（1または20）と、実行器（2または21）の求めに応じて実行許可情報を配布するソフト配布器（11）とからなり、ソフト配布器（11）から配布される実行許可情報の不正な使用を防止するためのソフトウェア実行制御システムであって、ソフト配布器（11）は、実行許可情報を保有しており、記録媒体（1または20）は、ソフトウェアを格納しており、実行器（2または21）は、自己の外部からは情報の読み出しおよび書き込みが困難な記憶領域（3または22）に、乱数を格納しており、実行許可情報の配布を求める際、実行器（2または21）は、ソフト配布器（11）に対して、格納している乱数を通知し、ソフト配布器（11）は、通知された乱数で実行許可情報を暗号化して、実行器（2または21）へ配布し、実行器（2または21）は、暗号化された実行許可情報の配布を受けると、配布された暗号化された実行許可情報を、格納している乱数で復号し、復号に連携して、格納している乱数を更新することを特徴としている。

【0051】上記のように、第17の発明は、ソフトウェアを実行する実行器と、実行器に接続され、かつ情報の読み出しおよび書き込みが可能な記録媒体と、実行許可情報を配布するソフト配布器とで構成されている。実行器は、当該実行器の外部からは情報の読み出しおよび書き込みが困難な記憶領域を備えており、この記憶領域に乱数を格納している。記録媒体は、ソフトウェアを格納しており、ソフト配布器は、実行許可情報を保有している。実行器は、実行許可情報を入手するために、格納している乱数をソフト配布器に対して通知する。ソフト配布器は、乱数の通知を受けると、保有している実行許可情報を、通知された乱数で暗号化して実行器に配布する。実行器は、最初、配布された暗号化された実行許可情報を、格納している乱数で復号して実行許可情報を求め、その後、格納している乱数を更新する。

【0052】このように、ソフト配布器から配布される実行許可情報を乱数で暗号化することにより、当該乱数を保有している実行器以外の実行器では、ソフトウェアを実行することができない。また、乱数は配布毎に更新されるため、実行許可情報が実行量に関する制限を含むものである場合に、正規の実行器で、コピーされた実行許可情報が繰り返し使用されるような不正を防ぐこともできる。

【0053】第18の発明は、ソフトウェアを実行する実行器（2または21）と、当該実行器（2または21）に情報伝達可能に接続され、かつ情報の読み出しおよび書き込みが可能な記録媒体（1または20）と、実行器（2または21）の求めに応じて実行許可情報を配布するソフト配布器（11）とからなり、実行器（2または21）が保有している実行許可情報に、ソフト配布器（11）から追加で配布される実行許可情報を加え、かつ実行許可情報の不正な使用を防止するためのソフトウェア実行制御システムであって、実行器（2または21）は、自己の外部からは情報の読み出しおよび書き込みが困難な記憶領域（3または22）に、第1および第2の乱数を格納しており、記録媒体（1または20）は、ソフトウェアおよび第1の暗号化された実行許可情報を格納しており、ソフト配布器（11）は、第2の実行許可情報を保有しており、実行器（2または21）は、第2の実行許可情報の配布を求める際に、ソフト配布器（11）に対して第2の乱数を通知し、ソフト配布器（11）は、通知された第2の乱数で第2の実行許可情報を暗号化して、実行器（2または21）に配布し、実行器（2または21）は、第2の暗号化された実行許可情報を受け取ると、受け取った第2の暗号化された実行許可情報を、格納している第2の乱数で復号して、第2の実行許可情報を求め、第2の暗号化された実行許可情報の復号に連携して、格納している第2の乱数を更新し、記録媒体（1または20）から第1の暗号化された実行許可情報を獲得して、第1の乱数で復号して、第1の実行許可情報を求め、第1の暗号化された実行許可情報の復号に連携して、格納している第1の乱数を更新し、求めた第1および第2の実行許可情報に基づいて、第3の実行許可情報を作成し、作成した第3の実行許可情報を、更新した第1の乱数で暗号化して、記録媒体（1または20）に格納することを特徴としている。

【0054】上記のように、第18の発明は、ソフトウェアを実行する実行器と、実行器に接続され、かつ情報の読み出しおよび書き込みが可能な記録媒体と、実行許可情報を配布するソフト配布器とで構成されている。実行器は、当該実行器の外部からは情報の読み出しおよび書き込みが困難な記憶領域を備えており、この記憶領域に第1および第2の乱数を格納している。記録媒体は、ソフトウェアおよび第1の実行許可情報を格納しており、ソフト配布器は、第2の実行許可情報を保有している。実行器は、第2の実行許可情報を入手するために、保有している第2の乱数をソフト配布器に対して通知する。ソフト配布器は、第2の乱数の通知を受けると、保有している実行許可情報を、通知された第2の乱数で暗号化して実行器に配布する。実行器は、最初、配布された、第2の暗号化された実行許可情報を、保有している第2の乱数で復号して第2の実行許可情報を求めるとと

もに、保有している第２の乱数を更新する。次に、実行器は、記録媒体から第１の暗号化された実行許可情報を獲得し、保有している第１の乱数で復号して第１の実行許可情報を求めるとともに、保有している第１の乱数を更新する。次に、実行器は、求めた第１および第２の実行許可情報に基づいて第３の実行許可情報を作成し、作成した第３の実行許可情報を、更新した第１の乱数で暗号化して記録媒体に格納する。これにより、実行器は、保有している実行許可情報にソフト配布器から入手した他の実行許可情報加えた新しい実行許可情報を作成し、その実行許可情報に基づいてソフトウェアを実行することができる。

【００５５】第１９の発明は、ソフトウェアを実行する第１および第２の実行器（２または２１）と、情報の読み出しおよび書き込みが可能な記録媒体（１または２０）とからなり、第１の実行器（２または２１）が保有している実行許可情報を第２の実行器（２または２１）へ譲渡し、かつ実行許可情報の不正な使用を防止するためのソフトウェア実行制御システムであって、第１の実行器（２または２１）は、自己の外部からは情報の読み出しおよび書き込みが困難な記憶領域（３または２２）に、乱数を格納しており、記録媒体（１または２０）は、ソフトウェアおよび暗号化された実行許可情報を格納しており、第１の実行器（２または２１）から第２の実行器（２または２１）に対して、第１の実行器（２または２１）が保有している実行許可情報を譲渡する際に、第１の実行器（２または２１）と第２の実行器（２または２１）とを情報伝達可能に接続し、第１の実行器（２または２１）は、自己の格納している乱数を第２の実行器（２または２１）に通知し、通知に連携して、自己の格納している乱数を更新し、第２の実行器（２または２１）は、乱数の通知を受けると、通知された乱数を、自己の外部からは情報の読み出しおよび書き込みが困難な記憶領域（３または２２）に格納することを特徴としている。

【００５６】上記のように、第１９の発明は、ソフトウェアを実行する第１および第２の実行器と、実行器に情報伝達可能に接続され、かつ情報の読み出しおよび書き込みが可能な記録媒体とで構成されている。第１および第２の実行器は、いずれも当該実行器の外部からは情報の読み出しおよび書き込みが困難な記憶領域を備えており、第１の実行器は、この記憶領域に乱数を格納している。記録媒体は、ソフトウェアおよび暗号化された実行許可情報を格納し、かつ第１の実行器に接続されている。今、第１の実行器は、保有している乱数で、暗号化された実行許可情報を復号して、ソフトウェアを実行することができる。第１の実行器が、この実行許可情報を第２の実行器に譲渡する際、第１の実行器は、最初、保有している乱数を第２の実行器に通知し、次に、保有している乱数を更新する。通知をうけて、第２の実行器は、通知された乱数を自己に備わる記憶領域に格納する。これにより、第２の実行器は、第１の実行器に接続されていた記録媒体を自己に接続し、記録媒体から暗号化された実行許可情報を獲得して復号し、ソフトウェアを実行することができる。

【００５７】第２０の発明は、ソフトウェアを実行する第１および第２の実行器（２または２１）と、それぞれの実行器（２または２１）に情報伝達可能に接続され、かつ情報の読み出しおよび書き込みが可能な第１および第２の記録媒体（１または２０）とからなり、第１の実行器（２または２１）が保有している実行許可情報の一部を第２の実行器（２または２１）に譲渡し、かつ実行許可情報の不正な使用を防止するためのソフトウェア実行制御システムであって、第１の実行器（２または２１）は、自己の外部からは情報の読み出しおよび書き込みが困難な記憶領域（３または２２）に、第１および第２の乱数を格納しており、第１の記録媒体（１または２０）は、ソフトウェアおよび暗号化された実行許可情報を格納しており、第２の記録媒体（１または２０）は、ソフトウェアを格納しており、第１の実行器（２または２１）から第２の実行器（２または２１）に対して、第１の実行器（２または２１）が保有している実行許可情報の一部を譲渡する際に、第１の実行器（２または２１）と第２の実行器（２または２１）とを情報伝達可能に接続し、第１の実行器（２または２１）は、第１の記録媒体（１または２０）から暗号化された実行許可情報を獲得して、格納している第１の乱数で復号し、復号に連携して、格納している第１の乱数を更新し、復号して求めた実行許可情報を、第１の実行許可情報と第２の実行許可情報とに分割し、分割して得た第１の実行許可情報を、更新した第１の乱数で暗号化して、第１の記録媒体（１または２０）に格納し、分割して得た第２の実行許可情報を、格納している第２の乱数で暗号化し、第２の乱数と、第２の暗号化された実行許可情報とを、第２の実行器（２または２１）に通知し、通知に連携して、格納している第２の乱数を更新し、第２の実行器（２または２１）は、第２の乱数と第２の暗号化された実行許可情報とを受け取ると、第２の乱数を自己の外部からは情報の読み出しおよび書き込みが困難な記憶領域（３または２２）に、第２の暗号化された実行許可情報を第２の記録媒体（１または２０）に、それぞれ格納することを特徴としている。

【００５８】上記のように、第２０の発明は、ソフトウェアを実行する第１および第２の実行器と、それぞれの実行器に情報伝達可能に接続され、かつ情報の書き込みおよび読み出しが可能な第１および第２の記録媒体とで構成されている。第１および第２の実行器は、いずれも当該実行器の外部からは情報の読み出しおよび書き込みが困難な記憶領域を備えており、第１の実行器は、この記憶領域に第１および第２の乱数を格納している。第１

の記録媒体はソフトウェアおよび暗号化された実行許可情報を格納し、第２の実行器はソフトウェアを格納している。今、第１の実行器は、保有している乱数で、暗号化された実行許可情報を復号して、ソフトウェアを実行することができる。第１の実行器は、この実行許可情報の一部を第２の実行器に譲渡する際、最初、第１の記録媒体から暗号化された実行許可情報を獲得し、保有している第１の乱数で復号して実行許可情報を求め、次に、保有している第１の乱数を更新するとともに、求めた実行許可情報を第１および第２の実行許可情報に分割する。次に、第１の実行器は、第１の実行許可情報を、更新した第１の乱数で暗号化して、第１の記録媒体に格納し、第２の実行許可情報を、保有している第２の乱数で暗号化して、第２の乱数と共に第２の実行器に通知する。この際、第１の実行器は、第２の乱数を更新する。通知を受けた第２の実行器は、第２の乱数を自己に備わる、情報の読み出しおよび書き込みが困難な記憶領域へ、第２の暗号化された実行許可情報を第２の記録媒体へ、それぞれ格納する。これにより、分割して得られた、第１の暗号化された実行許可情報は第１の実行器が、第２の暗号化された実行許可情報は第２の実行器が、それぞれ復号することができる。

【００５９】第２１の発明は、ソフトウェアを実行するにはソフト鍵を必要とし、かつソフト鍵の不正な使用を防止するためのソフトウェア実行制御システムであって、暗号化されたソフトウェアおよび暗号化されたソフト鍵を格納し、かつ情報の読み出しおよび書き込みが可能な記録媒体（１）が、ソフトウェアを実行する実行器（２）に情報伝達可能に接続され、実行器（２）は、乱数を格納し、かつ自己の外部からは情報の読み出しおよび書き込みが困難な乱数格納手段（３）と、記録媒体（１）から暗号化されたソフト鍵を獲得して、乱数格納手段（３）から取得した乱数で復号する第１の復号手段（４）と、記録媒体（１）から暗号化されたソフトウェアを獲得して、第１の復号手段（４）の復号によって得られたソフト鍵で復号する第２の復号手段（６）と、第２の復号手段（６）の復号によって得られたソフトウェアを実行するソフト実行手段（７）と、ソフトウェアの実行に関連して、乱数格納手段（３）に格納された乱数を更新する乱数更新手段（９）と、第１の復号手段（４）の復号によって得られたソフト鍵を、更新された乱数で暗号化して、記録媒体（１）に格納する暗号化手段（１０）とを備えている。

【００６０】上記のように、第２１の発明は、ソフトウェアを実行する実行器と、暗号化されたソフトウェアおよび暗号化されたソフト鍵を格納している記録媒体とで構成されている。ソフトウェアを実行する際、実行器に備わる第１の復号手段は、記録媒体から暗号化されたソフト鍵を獲得し、乱数格納手段に格納された乱数で復号してソフト鍵を求める。次に、第２の復号手段は、記録媒体から暗号化されたソフトウェアを獲得し、求められたソフト鍵で復号してソフトウェアを得る。次に、ソフト実行手段は、得られたソフトウェアを実行する。この際、乱数更新手段は、乱数格納手段に格納された乱数を更新する。続いて、暗号化手段は、更新された乱数でソフト鍵を暗号化して、記録媒体に格納する。このように、ソフト鍵を暗号化するための鍵を乱数とし、実行毎に更新することで、鍵を第三者に知られても、暗号化されたソフト鍵を復号できないようにすることができる。

【００６１】第２２の発明は、実行回数が所定の条件を満足する場合に、ソフトウェアを実行し、かつ当該実行回数の不正な使用を防止するためのソフトウェア実行制御システムであって、ソフトウェアおよび暗号化された実行回数を格納し、かつ情報の読み出しおよび書き込みが可能な記録媒体（１）が、ソフトウェアを実行する実行器（２）に情報伝達可能に接続され、実行器（２）は、乱数を格納し、かつ自己の外部からは情報の読み出しおよび書き込みが困難な乱数格納手段（３）と、記録媒体（１）から暗号化された実行回数を獲得して、乱数格納手段（３）から取得した乱数で復号する復号手段（４）と、復号手段（４）の復号によって得られた実行回数が、所定の条件を満足するか否かを検査し、所定の条件を満足する場合に、ソフトウェアの実行を指示する実行回数検査手段（５）と、実行回数検査手段（５）からの指示に応答して、ソフトウェアを実行するソフト実行手段（７）と、ソフトウェアの実行にともなって、復号によって得られた実行回数を更新する実行回数更新手段（８）と、ソフトウェアの実行に連携して、乱数格納手段（３）に格納された乱数を更新する乱数更新手段（９）と、更新された実行回数情報を、更新された乱数で暗号化して、記録媒体（１）に格納する暗号化手段（１０）とを備えている。

【００６２】上記のように、第２２の発明は、ソフトウェアを実行する実行器と、ソフトウェアおよび暗号化された実行回数を格納している記録媒体とで構成されている。最初、実行器に備えられた復号手段は、記録媒体から、暗号化された実行回数を獲得して、乱数格納手段に格納された乱数で復号して実行回数を求める。次に、実行回数検査手段は、求められた実行回数が所定の条件を満足するか否かを検査し、満足すれば、ソフト実行手段に対して、ソフトウェアの実行を指示する。ソフト実行手段は、実行回数検査手段の指示を受けてソフトウェアを実行し、乱数更新手段は、ソフトウェアの実行にともなって、乱数を更新する。次に、暗号化手段は、更新された実行回数を更新された乱数で暗号化して、記録媒体に格納する。このように、実行回数を乱数で暗号化し、実行毎に乱数を更新することにより、コピーされた、暗号化された実行回数を復号不能にすることができる。また、更新された実行回数を記録媒体へ書き込むのを妨害する攻撃を防止することもできる。

【００６３】第２３の発明は、実行回数が所定の条件を満足する場合に、ソフト鍵で復号して得られたソフトウェアを実行し、かつ実行回数およびソフト鍵の不正な使用を防止するためのソフトウェア実行制御システムであって、暗号化されたソフトウェアおよび暗号化されたソフト鍵／実行回数を格納し、かつ情報の読み出しおよび書き込みが可能な記録媒体（１）が、ソフトウェアを実行する実行器（２）に情報伝達可能に接続され、実行器（２）は、乱数を格納し、かつ自己の外部からは情報の読み出しおよび書き込みが困難な乱数格納手段（３）と、記録媒体（１）から暗号化されたソフト鍵／実行回数を獲得して、乱数格納手段（３）から取得した乱数で復号する第１の復号手段（４）と、記録媒体（１）から暗号化されたソフトウェアを獲得して、第１の復号手段（４）の復号によって得られたソフト鍵で復号する第２の復号手段（６）と、第１の復号手段（４）の復号によって得られた実行回数が、所定の条件を満足するか否かを検査し、所定の条件を満足する場合に、ソフトウェアの実行を指示する実行回数検査手段（５）と、実行回数検査手段（５）からの指示に応答して、第２の復号手段（６）の復号によって得られたソフトウェアを実行するソフト実行手段（７）と、ソフトウェアの実行に伴って、復号によって得られた実行回数を更新する実行回数更新手段（８）と、ソフトウェアの実行に連携して、乱数格納手段（３）に格納された乱数を更新する乱数更新手段（９）と、復号によって得られたソフト鍵と更新された実行回数とを、更新された乱数で暗号化して記録媒体（１）に格納する暗号化手段（１０）とを備えている。

【００６４】上記のように、第２３の発明は、ソフトウェアを実行する実行器と、ソフトウェアおよび暗号化されたソフト鍵／実行回数を格納している記録媒体とで構成されている。最初、実行器に備わる第１の復号手段は、記録媒体から暗号化されたソフト鍵／実行回数を獲得し、乱数格納手段に格納された乱数で復号して、ソフト鍵および実行回数を求める。次に、第２の復号手段が、記録媒体から暗号化されたソフトウェアを獲得して、求められたソフト鍵で復号し、実行回数検査手段は、求められた実行回数が所定の条件を満足するか否かを検査し、満足する場合にソフト実行手段に対してソフトウェアの実行を指示する。ソフト実行手段は、実行回数検査手段の指示を受けて、ソフトウェアを実行する。ソフトウェアの実行に伴って、実行回数更新手段が実行回数を更新し、乱数更新手段は乱数格納手段に格納された乱数を更新する。続いて、暗号化手段は、ソフト鍵および更新された実行回数を、更新された乱数で暗号化して記録媒体に格納する。

【００６５】このように、実行回数を乱数で暗号化して実行毎に乱数を更新することにより、コピーされた、暗号化された実行回数を復号することができないようにし、また、更新された実行回数を記録媒体に書き込む書き込み妨害する攻撃を防止することができる。また、ソフトウェアをソフト鍵で暗号化し、さらにソフト鍵を乱数で暗号化して、ソフトウェアの実行毎に乱数を更新することで、ソフト鍵が第三者に知られることによるソフトウェアの不正な使用を防止することもできる。

【００６６】第２４の発明は、実行回数が所定の条件を満足する場合に、ソフト鍵で復号して得られたソフトウェアを実行し、かつソフト鍵および実行回数の不正な使用を防止するためのソフトウェア実行制御システムであって、複数の、暗号化されたソフトウェア、暗号化されたソフト鍵／実行回数および暗号化された補助鍵が格納され、かつ情報の読み出しおよび書き込みが可能な記録媒体（２０）が、ソフトウェアを実行する実行器（２１）に情報伝達可能に接続され、実行器（２１）は、乱数を格納し、かつ自己の外部からは情報の読み出しおよび書き込みが困難な乱数格納手段（２２）と、記録媒体（２０）から、当該ソフトウェアに専用の暗号化された補助鍵を獲得して、乱数格納手段（２２）から取得した乱数で復号する第１の復号手段（２３）と、記録媒体（２０）から、当該ソフトウェアに専用の暗号化されたソフト鍵／実行回数を獲得して、第１の復号手段（２３）の復号によって得られた補助鍵で復号する第２の復号手段（２４）と、記録媒体（２０）から暗号化されたソフトウェアを獲得して、第２の復号手段（２４）の復号によって得られたソフト鍵で復号する第３の復号手段（２５）と、第２の復号手段（２４）の復号によって得られた実行回数が、所定の条件を満足するか否かを検査し、所定の条件を満足する場合に、当該ソフトウェアの実行を指示する実行回数検査手段（２６）と、実行回数検査手段（２６）からの指示に応答して、第３の復号手段（２５）の復号によって得られたソフトウェアを実行するソフト実行手段（２９）とソフトウェアの実行に伴って、第２の復号手段（２４）の復号によって得られた実行回数を更新する実行回数更新手段（２７）と、第２の復号手段（２４）の復号によって得られたソフト鍵と、実行回数更新手段（２７）によって更新された実行回数とを、第１の復号手段（２３）の復号によって得られた補助鍵で暗号化して、記録媒体（２０）に格納する第１の暗号化手段（２８）と、所定のタイミングで、記録媒体（２０）から全ての暗号化された補助鍵を獲得して、乱数格納手段（２２）から取得した乱数で復号する第４の復号手段（３０）と、第４の復号手段（３０）の復号に連携して、乱数格納手段（２２）に格納された乱数を更新する乱数更新手段（３１）と、第４の復号手段（３０）の復号によって得られた補助鍵を、乱数更新手段（３１）によって更新された乱数で暗号化して、記録媒体（２０）に格納する第２の暗号化手段（３２）とを備えている。

【００６７】上記のように、第２４の発明は、ソフトウ

ェアを実行する実行器と、複数の、ソフトウェア、暗号化されたソフト鍵／実行回数および暗号化された補助鍵を格納している記録媒体とで構成されている。実行器に備わる第１の復号手段は、最初、記録媒体から当該ソフトウェアに対応する暗号化された補助鍵を獲得し、乱数格納手段に格納された乱数で復号して、補助鍵を求める。次に、第２の復号手段は、記録媒体から、暗号化されたソフト鍵実行回数を獲得し、求められた補助鍵で復号してソフト鍵および実行回数を得る。次に、第３の復号手段が、記録媒体から暗号化されたソフトウェアを獲得し、得られたソフト鍵で復号してソフトウェアを求め、実行回数検査手段は、求められた実行回数が所定の条件を満足するか否かを検査し、満足する場合にソフト実行手段に対してソフトウェアの実行を指示する。ソフト実行手段は、実行回数検査手段の指示を受けて、求められたソフトウェアを実行する。ソフトウェアの実行に伴って、実行回数更新手段は実行回数を更新する。続いて、第１の暗号化手段は、更新された実行回数を、求められた補助鍵で暗号化して記録媒体に格納する。第４の復号手段は、所定のタイミングで、記録媒体から全ての暗号化された補助鍵を獲得して、乱数格納手段に格納された乱数で復号して補助鍵を求める。乱数更新手段は、第４の復号手段の復号に連携して、乱数格納手段に格納された乱数を更新する。第２の暗号化手段は、第４の復号手段の復号によって得られた補助鍵を、更新された乱数で暗号化して記録媒体に格納する。

【００６８】このように、複数のソフトウェアを扱う場合には、それぞれのソフト鍵および実行回数を専用の補助鍵で暗号化し、さらに、これらの補助鍵を乱数で暗号化する。そして、所定のタイミングで乱数を更新することにより、コピーされた、暗号化された実行回数を復号することができないようにし、また、更新された実行回数を記録媒体に書き込むのを妨害する攻撃を防ぐことができる。また、ソフト鍵が第三者に知られることによるソフトウェアの不正な使用を防止することもできる。さらに、実行器の外部からの情報の読み出しおよび書き込みが困難な記憶領域は、ソフトウェアの数に関わらず、１個の乱数を格納する大きさの領域があればよく、コストを低く押さえることもできる。

【００６９】

【発明の実施の形態】

（第１の実施形態）図１は、本発明の第１の実施形態に係るソフトウェア実行制御システムの構成を示すブロック図である。図１において、本システムは、ソフトウェアを格納する記録媒体１と、ソフトウェアを実行する実行器２とを備えている。実行器２は、乱数格納部３と、第１の復号部４と、実行回数検査部５と、第２の復号部６と、ソフト実行部７と、実行回数更新部８と、乱数更新部９と、暗号部１０とを含む。

【００７０】図２は、図１のソフトウェア実行制御システムの動作を示すフローチャートである。以下には、図２を用いて、図１に示すシステムの動作を説明する。今、乱数格納部３には、乱数Ｒが格納されており、記録媒体１には、あるソフトウェアＳｏｆｔＡをソフト鍵Ｋで暗号化した暗号化ソフトＥ（Ｋ，ＳｏｆｔＡ）と、ソフト鍵Ｋおよび実行回数ｎを乱数Ｒで暗号化した暗号化ソフト鍵／実行回数Ｅ（Ｒ，（Ｋ，ｎ））とが格納されている。記録媒体１を実行器２に接続して、ソフトウェアＳｏｆｔＡを実行する際に、実行器２は、記録媒体１から暗号化ソフトＥ（Ｋ，ＳｏｆｔＡ）と暗号化ソフト鍵／実行回数Ｅ（Ｒ，（Ｋ，ｎ））とを獲得する（ステップＳ１０１）。次に、実行器２内の第１の復号部４は、暗号化ソフト鍵／実行回数Ｅ（Ｒ，（Ｋ，ｎ））を乱数Ｒで復号して、ソフト鍵Ｋおよび実行回数ｎを求める（ステップＳ１０２）。次に、実行回数検査部５は、求めた実行回数ｎが１以上であるか否かを検査し（ステップＳ１０３）、ｎが１以上であればソフト実行部７に対して、実行ＯＫを通知し、ｎが０であれば、システムの動作を終了させる。ｎが１以上の場合、第２の復号部６は、暗号化ソフトＥ（Ｋ，ＳｏｆｔＡ）を、求めたソフト鍵Ｋで復号してソフトウェアＳｏｆｔＡを求める（ステップＳ１０４）。次に、ソフト実行部７は、実行回数検査部５から実行ＯＫの通知を受けて、求めたソフトウェアＳｏｆｔＡを実行する（ステップＳ１０５）。ソフトウェアＳｏｆｔＡを実行すると、実行回数更新部８は、実行回数ｎを１減少してｎ′（＝ｎ－１）に更新し（ステップＳ１０６）、乱数更新部９は、乱数格納部３の乱数ＲをＲ′に更新する（ステップＳ１０７）。次に、暗号部１０は、更新された乱数Ｒ′で、ソフト鍵Ｋおよび実行回数ｎ′を暗号化し（ステップＳ１０８）、この更新された暗号化鍵／実行回数Ｅ（Ｒ′，（Ｋ，ｎ′））を記録媒体１に再び格納する（ステップＳ１０９）。

【００７１】ここで、記録媒体１および実行器２は、以下の条件を満たしているものとする。

（１）記録媒体は、情報の読み出しおよび書き込みができる。

（２）記録媒体と実行器との間では、情報の読み出しおよび書き込みができる。

（３）実行器内の、動作中の各部の間を移動する情報は、実行器の外部からは、読み出しおよび書き込みはできない。また、各部で動作中に求められ、利用される情報は、実行器の内部のＲＡＭに格納して利用し、動作後には消去される。

（４）実行器内の乱数格納部は、実行制御を行なう特別なシステムプログラム以外からは、情報の読み出しおよび書き込みはできない。

【００７２】このとき、図１のソフトウェア実行制御システムは、次のようにして第１の攻撃を防ぐことができる。実行回数ｎが０になる前に、記録媒体１をコピーし

ておく。コピーの記録媒体には、暗号化ソフトＥ（Ｋ，ＳｏｆｔＡ）、およびコピーした時点での暗号化ソフト鍵／実行回数Ｅ（Ｒ，（Ｋ，ｎ））が格納されている。この暗号化ソフト鍵／実行回数Ｅ（Ｒ，（Ｋ，ｎ））を復号するには、暗号鍵である乱数Ｒが必要である。記録媒体１に格納された実行許可情報の実行回数ｎが少なくなった時点で、コピーに差し替えて再び実行を試みても、実行器２内の乱数は、すでにＲとは異なる値に更新されており、コピーに格納されている暗号化ソフト鍵／実行回数Ｅ（Ｒ，（Ｋ，ｎ））を復号してソフト鍵Ｋを得ることができず、従って、ソフトウェアＳｏｆｔＡを実行することができない。

【００７３】同時に、図１のソフトウェア実行制御システムは、次のようにして第２の攻撃を防ぐことができる。更新された暗号化ソフト鍵／実行回数Ｅ（Ｒ′，（Ｋ，ｎ′））の、記録媒体１への書き込みを、記録媒体と実行器との間で妨害する。実行器２内の乱数はＲからＲ′に更新されているのにも関わらず、記録媒体１には更新前の乱数Ｒで暗号化された暗号化ソフト鍵／実行回数Ｅ（Ｒ，（Ｋ，ｎ））が格納されたままになっている。このため、次に実行を試みても、乱数Ｒ′では暗号化ソフト鍵／実行回数Ｅ（Ｒ，（Ｋ，ｎ））を復号することができず、従って、ソフトウェアＳｏｆｔＡを実行することができない。

【００７４】なお、本実施形態では、実行可能な回数を実行制御のためのパラメータとし、これを１ずつ減少していく構成にしたが、実行の上限回数を設定しておき、実行した回数をパラメータとして、これを１づつ増加していく構成にしてもよい。あるいは、実行時間で制御することもできる。このように、実行制御のためのパラメータは、実行の分量を表すことのできる量であればよい。また、ソフトウェアの実行回数だけでなく、１つのソフトウェアの中で、項目を限定して、実行回数を制限するよう拡張することもできる。もちろん、コンピュータソフトウェアだけでなく、ゲームやその他さまざまなマルチメディアソフトウェアを対象としてもよい。

【００７５】ところで、本実施形態では、ソフトの実行毎に乱数を更新しているが、数回の実行毎に乱数を更新するようにすれば、実行制御に要する処理の負荷を軽減することができる。この場合には、同じ乱数Ｒを使用している間は上記第１および第２の攻撃が可能であるが、乱数の更新の頻度を適切に設定することにより、これらを有効に防止することができる。

【００７６】また、本実施形態において、乱数Ｒの更新の間隔をまちまちにして、かつ、ユーザに秘密にすることにより、更新の頻度に対する第１および第２の攻撃の防止効果を高めることができる。

【００７７】さらにまた、本実施形態において、乱数を格納する記憶領域を、実行器２にではなく、記録媒体１に備えることにより、実行器を限定することなく、ソフトウェアの実行回数だけを制御するようにすることもできる。

【００７８】あるいは、本実施形態において、記録媒体１に代えて、読み出し専用の第１の記録媒体と、読み出しおよび書き込みが可能な第２の記録媒体とを備えるようにし、暗号化ソフトは第１の記録媒体に、暗号化ソフト鍵／実行回数は第２の記録媒体に、それぞれ格納するようにすることもできる。この際には、例えば、第１の記録媒体はＣＤ－ＲＯＭ、第２の記録媒体は拡張メモリを用いればよい。

【００７９】図３は、本実施形態に係るソフトウェア実行制御システムの、実行器がソフト配布器からソフトウェアの配布を受ける際の構成を示すブロック図である。図３において、本システムは、記録媒体１と、実行器２と、ソフト配布器１１とを備えている。ソフト配布器１１は、暗号部１２を備えており、実行器２は、図１におけるものに、さらに、第３の復号部１３が追加されているが、ここでは、必要な部分だけが表示されている。

【００８０】図４は、図３に示すシステムの動作を示すフローチャートである。図４を用いて、図３に示すシステムの動作を説明する。実行器２内の乱数格納部３には、実行制御のための乱数Ｒに加えて、実行許可情報の移動を制御するための乱数ｒが格納されている。実行器２は、ソフトウェアＳｏｆｔＡの配布を注文する際に、ソフト配布器１１に対して乱数ｒを通知する（ステップＳ２０１）。乱数ｒを通知されたソフト配布器１１は、最初、暗号部１２において、ソフト鍵Ｋおよび実行回数ｎをこの乱数ｒで暗号化する。次に、ソフト配布器１１は、この暗号化ソフト鍵／実行回数Ｅ（ｒ，（Ｋ，ｎ））と、暗号化ソフトＥ（Ｋ，ＳｏｆｔＡ）とを、実行器２に対して、記録媒体１に格納して送付、または通信回線を介して送信する（ステップＳ２０２）。これらを受け取った実行器２は、まず、第３の復号部１３において、乱数格納部３に格納した乱数ｒで暗号化ソフト鍵／実行回数Ｅ（ｒ，（Ｋ，ｎ））を復号して、ソフト鍵Ｋおよび実行回数ｎを得る（ステップＳ２０３）。この際、乱数更新部９は、乱数格納部３に格納された乱数ｒをｒ′に更新する（ステップＳ２０４）。続いて、実行器２は、暗号部１０において、乱数格納部３に格納された乱数Ｒで、ソフト鍵Ｋおよび実行回数ｎを暗号化し（ステップＳ２０５）、この暗号化ソフト鍵／実行回数Ｅ（Ｒ，（Ｋ，ｎ））を記録媒体１に格納する（ステップＳ２０６）。

【００８１】上記のようにして配布されたソフトウェアは、乱数ｒを保有しているもの以外の実行器では、実行することができない。また、暗号鍵として乱数ｒを用いると、ソフト購入毎に乱数ｒが更新されるため、一度入手した実行許可情報をコピーして繰り返し使用されるのを防ぐことができる。

【００８２】なお、上記の手順では、実行器２はソフト

配布器１１に乱数ｒをそのまま通知しているが、乱数ｒを暗号化することでより一層安全性を高めることができる。また、認証や署名の情報を付加すると、さらに安全性が向上する。

【００８３】ところで、第１の実施形態において、複数の実行器の間で、あるいはソフト配布器と実行器との間で、実行許可情報の移動を伴う次の３つの場合についてのソフトウェア実行制御方法を説明する。

（１）ソフトウェアＳｏｆｔＡをＮ回実行することのできる実行許可情報を、追加で購入する場合。

実行器２は、乱数Ｒおよびｒを内部に保有している。まず、実行器２は、乱数ｒをソフト配布器１１に通知する。ソフト配布器１１は、ソフト鍵Ｋおよび実行回数Ｎを、通知された乱数ｒで暗号化し、実行器２に送付する。実行器２は、送付された暗号化ソフト鍵／実行回数Ｅ（ｒ，（Ｋ，Ｎ））を乱数ｒで復号してソフト鍵Ｋおよび実行回数Ｎを得ると同時に、自己の内部の乱数ｒをｒ′に更新する。次に、実行器２は、記録媒体１から、先に購入した暗号化ソフト鍵／実行回数Ｅ（Ｒ，（Ｋ，ｎ））を獲得し、乱数Ｒで復号してソフト鍵Ｋおよび実行回数ｎを求めるとともに、乱数ＲをＲ′に更新する。続いて、実行器２は、ｎにＮを加算した実行回数ｎ＋Ｎとソフト鍵Ｋとを、更新した乱数Ｒ′で暗号化し、この暗号化ソフト鍵／実行回数Ｅ（Ｒ′，（Ｋ，ｎ＋Ｎ））を記録媒体１に格納する。このようにして、実行器２は、更にｎ回実行する許可を得る。

【００８４】（２）第１の実行器が所有する実行許可情報を、第２の実行器に譲渡する場合。

内部に乱数Ｒを保有している第１の実行器に、第２の実行器を接続する。第１の実行器は、乱数Ｒを第２の実行器に通知すると同時に、自己の保有する乱数ＲをＲ′に更新する。第２の実行器は、第１の実行器から通知された乱数Ｒを内部に格納する。第２の実行器は、記録媒体に格納された暗号化ソフト鍵／実行回数Ｅ（Ｒ，（Ｋ，ｎ））を復号して、ソフトウェアＳｏｆｔＡを実行することができる。このようにして、第１の実行器の保有していた実行許可情報は、第２の実行器に譲渡され、第１の実行器は実行する権利を失う。

【００８５】（３）第１の実行器が所有する実行許可情報を分割して、その一部を第２の実行器に譲渡する場合。

第１の実行器は、内部に、乱数Ｒおよびｒを保有している。第１の実行器は、記録媒体から獲得した実行許可情報を乱数Ｒで復号してソフト鍵Ｋおよび実行回数ｎを得ると、ｎをｎ１とｎ２とに分割する。この際、第１の実行器は、乱数ＲをＲ′に更新する。次に、ソフト鍵Ｋおよび実行回数ｎ１を、更新された乱数Ｒ′により暗号化して、この暗号化ソフト鍵／実行回数Ｅ（Ｒ′，（Ｋ，ｎ１））を、自己と接続された記録媒体に格納する。同時に、第１の実行器は、乱数ｒでソフト鍵Ｋおよび実行回数ｎ２を暗号化し、この暗号化ソフト鍵／実行回数Ｅ（ｒ，（Ｋ，ｎ２））と乱数ｒとを第２の実行器に通知した後、自己の内部の乱数ｒをｒ′に更新する。第２の実行器は、これらを受け取ると、乱数ｒを自己の内部に、暗号化ソフト鍵／実行回数Ｅ（ｒ，（Ｋ，ｎ２））を自己に接続された記録媒体に、それぞれ格納する。このようにして、第１の実行器の保有していた、ソフトウェアＳｏｆｔＡをｎ回実行することのできる実行許可情報のうち、ｎ２回分の実行許可情報が第２の実行器に譲渡され、第１の実行器には、ｎ１回分の実行許可情報が残される。

【００８６】なお、本実施形態では、ソフトウェアをソフト鍵で暗号化する構成になっているが、ソフトウェアを暗号化しない構成でも、目的を達成することができる。

【００８７】ところで、本実施形態のソフトウェア実行制御システムは、一つの実行器につき一つのソフトウェアを扱っている。本システムにおいて、一つの実行器で複数のソフトを扱えるようにするには、実行制御のための乱数をソフト毎に用意し、実行器の内部に格納しておく必要がある。従って、実行器に、複数の乱数を格納可能な大きさの記憶領域を設けることが必要である。そこで、次に述べる第２の実施形態では、一つの実行器で同時に複数のソフトを扱う場合にも、当該実行器に、１つの乱数だけを格納可能な記憶領域を設ければよいようなソフトウェア実行制御システムを提供する。

【００８８】（第２の実施形態）図５は、本発明の第２の実施形態に係るソフトウェア実行制御システムの構成を示すブロック図である。図５において、本システムは、ソフトウェアを格納する記録媒体２０と、ソフトウェアを実行する実行器２１とを備えている。実行器２１は、乱数格納部２２と、第１の復号部２３と、第２の復号部２４と、第３の復号部２５と、実行回数検査部２６と、実行回数更新部２７と、第１の暗号部２８と、ソフト実行部２９とを含む。

【００８９】図６は、図５のソフトウェア実行制御システムの動作を示すフローチャートである。図６を用いて、図５に示すシステムの動作を説明する。記録媒体２０には、ソフトウェアＳｏｆｔＡに関する情報として、暗号化ソフトＥ（ＫＡ，ＳｏｆｔＡ）と、暗号化ソフト鍵／実行回数Ｅ（ＲＡ，（ＫＡ，ｎＡ））と、暗号化補助鍵Ｅ（Ｒ，ＲＡ）とが、ソフトウェアＳｏｆｔＢに関する情報として、暗号化ソフトＥ（ＫＢ，ＳｏｆｔＢ）と、暗号化ソフト鍵／実行回数Ｅ（ＲＢ，（ＫＢ，ｎＢ））と、暗号化補助鍵Ｅ（Ｒ，ＲＢ）とが、格納されている。ここで、ＲＡおよびＲＢは、それぞれソフトウェアＳｏｆｔＡおよびソフトウェアＳｏｆｔＢに専用の補助鍵であり、Ｅ（Ｒ，ＲＡ）およびＥ（Ｒ，ＲＢ）は、これらをそれぞれ乱数Ｒで暗号化したものである。

【００９０】乱数格納部２２は、図１における乱数格納

部３と同様に、読み出しおよび書き込みの困難な領域であり、乱数Ｒを格納している。実行器２１は、記録媒体２０からソフトウェアＳｏｆｔＡに関する情報を獲得すると（ステップＳ３０１）、第１の復号部２３において、乱数Ｒによって、暗号化補助鍵Ｅ（Ｒ，ＲＡ）を復号し、補助鍵ＲＡを得る（ステップＳ３０２）。続いて、実行器２１は、第２の復号部２４において、この補助鍵ＲＡにより、暗号化ソフト鍵／実行回数Ｅ（ＲＡ，（ＫＡ，ｎＡ））を復号し、ソフト鍵ＫＡおよび実行回数ｎＡを得る（ステップＳ３０３）。さらに、実行器２１は、第３の復号部２５において、ソフト鍵ＫＡにより、暗号化ソフトＥ（ＫＡ，ＳｏｆｔＡ）を復号し、ソフトウェアＳｏｆｔＡを得る（ステップＳ３０４）。同時に、実行器２１は、実行回数検査部２６において、実行回数ｎＡが１以上であるか否かを検査し（ステップＳ３０５）、ｎＡが１以上であればソフト実行部２９に対して実行ＯＫを通知し、この通知を受けて、ソフト実行部２９はソフトウェアＳｏｆｔＡを実行する（ステップＳ３０６）。この後、実行回数更新部２７は、実行回数ｎＡを１減少してｎＡ′（＝ｎＡ－１）に更新する（ステップＳ３０７）。実行回数ｎＡ′は、第１の暗号部２８において、ソフト鍵ＫＡと共に補助鍵ＲＡで暗号化され（ステップＳ３０８）、この暗号化ソフト鍵／実行回数Ｅ（ＲＡ，（ＫＡ，ｎＡ′））が、記録媒体２０に再び格納される（ステップＳ３０９）。ソフトウェアＳｏｆｔＢについても、同様にして実行される。

【００９１】図７は、本実施形態において、所定のタイミングで乱数Ｒを更新する際の、ソフトウェア実行システムの構成を示すブロック図である。図７において、記録媒体２０は、図５におけるものと同様の情報を格納している。実行器２１は、図５におけるものに加えて、第４の復号部３０と、乱数更新部３１と、第２の暗号部３２とを更に含むが、図には必要な部分だけが表示されている。

【００９２】図８は、図７に示すシステムの、所定のタイミングで乱数Ｒを更新する際の動作を示すフローチャートである。図８を用いて、図７に示すシステムの動作を説明する。実行器２１は、記録媒体２０から暗号化補助鍵Ｅ（Ｒ，ＲＡ）およびＢ（Ｒ，ＲＢ）を獲得すると（ステップＳ４０１）、第４の復号部３０において乱数Ｒで復号して、補助鍵ＲＡおよびＲＢを得る（ステップＳ４０２）。この際、実行器２１は、乱数更新部３１において、乱数格納部２２に格納された乱数ＲをＲ′に更新する（ステップＳ４０３）。続いて、実行器２１は、第２の暗号部３２において、乱数Ｒ′で補助鍵ＲＡおよびＲＢをそれぞれ暗号化し（ステップＳ４０４）、これらの暗号化補助鍵Ｅ（Ｒ′，ＲＡ）およびＥ（Ｒ′，ＲＢ）を記録媒体２０に再び格納する（ステップＳ４０５）。

【００９３】このように、第２の実施形態では、ソフト鍵および実行回数を暗号化するための各ソフトウェア毎の補助鍵と、それらの補助鍵を束ねてそれぞれ暗号化するための乱数Ｒとを用意して、乱数格納部には乱数Ｒだけを格納するようにしている。このため、読み出しおよび書き込みのできない領域の大きさを最小にすることができて、実現コストも低く抑えることができる。

【００９４】なお、乱数Ｒの更新は、できるだけ頻繁に行なうほうが、先に述べた第１および第２の攻撃に対する防御効果は大きいが、記録媒体に格納されているソフトウェアの数が多い場合には、特に処理の負荷が大きくなってしまう。そのため、更新の頻度は、トレードオフを考慮して決定する。また、第１の実施形態でも述べた通り、更新の間隔を可変にし、かつ秘密にすることも、安全性を高める上で有効である。

【００９５】また、本実施形態では、ソフトウェアをソフト鍵で暗号化する構成になっているが、ソフトウェアを暗号化しない構成でも、目的を達成することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係るソフトウェア実行制御システムの、ソフトウェアを実行する際の構成を示すブロック図である。

【図２】図１のソフトウェア実行制御システムの動作を示すフローチャートである。

【図３】本発明の第１の実施形態に係るソフトウェア実行制御システムの、実行器がソフト配布器からソフトウェアの配布を受ける際の構成を示すブロック図である。

【図４】図３のソフトウェア実行制御システムの動作を示すフローチャートである。

【図５】本発明の第２の実施形態に係るソフトウェア実行制御システムの、ソフトウェアを実行する際の構成を示すブロック図である。

【図６】図５のソフトウェア実行制御システムの動作を示すフローチャートである。

【図７】本発明の第２の実施形態に係るソフトウェア実行制御システムの、乱数を更新する際の構成を示すブロック図である。

【図８】図７のソフトウェア実行制御システムの動作を示すフローチャートである。

【図９】第１の従来例に係るソフトウェア実行制御システムの構成を示すブロック図である。

【図１０】第２の従来例に係るソフトウェア実行制御システムの構成を示すブロック図である。

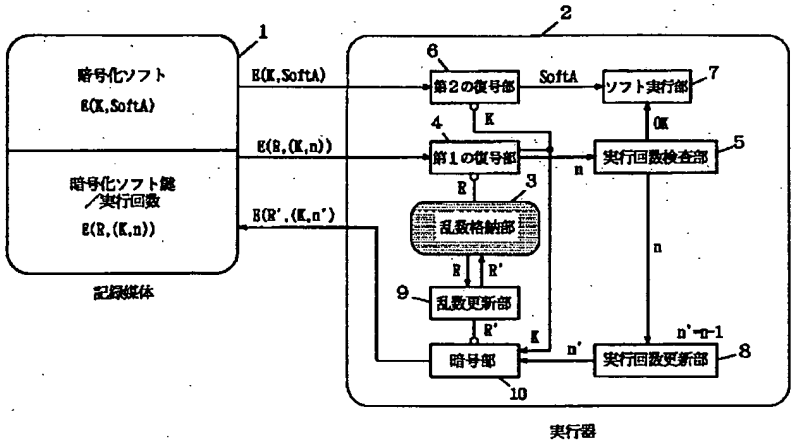
【図１１】第３の従来例に係るソフトウェア実行制御システムの構成を示すブロック図である。

【符号の説明】

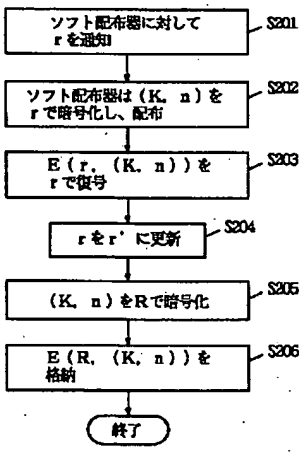
１、２０、１０３、１１０　記録媒体
２、２１、１０１、１１１　実行器
３、２２　乱数格納部
４、２３　第１の復号部

5、26、106、119　実行回数検査部
6、24　第2の復号部
7、29　ソフト実行部
8、27、107、118　実行回数更新部
9、31　乱数更新部
10、108　暗号部
11　ソフト配布器
13、25　第3の復号部
28．第1の暗号部
30　第4の復号部
32　第2の暗号部
102、113　固有鍵格納部
104、105、114、117　復号部
112　コプロセッサ
115　ソフト鍵格納部
116　実行回数格納部

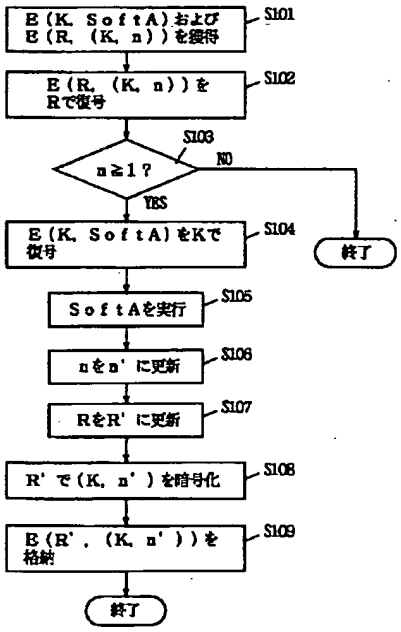
【図1】



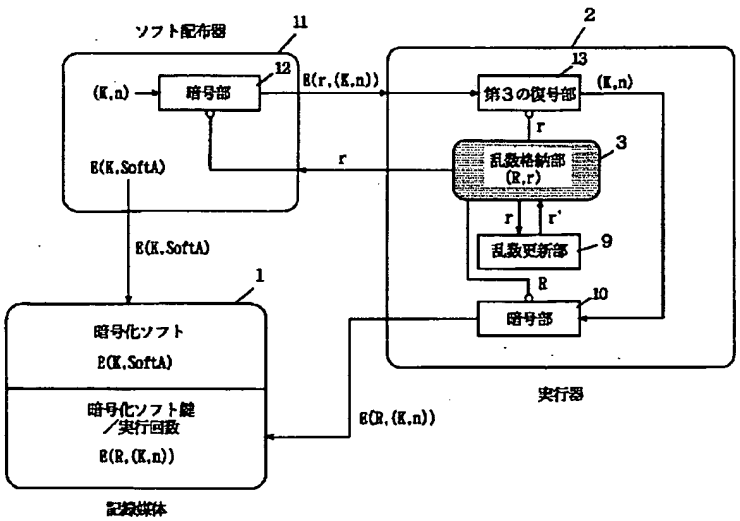
【図4】



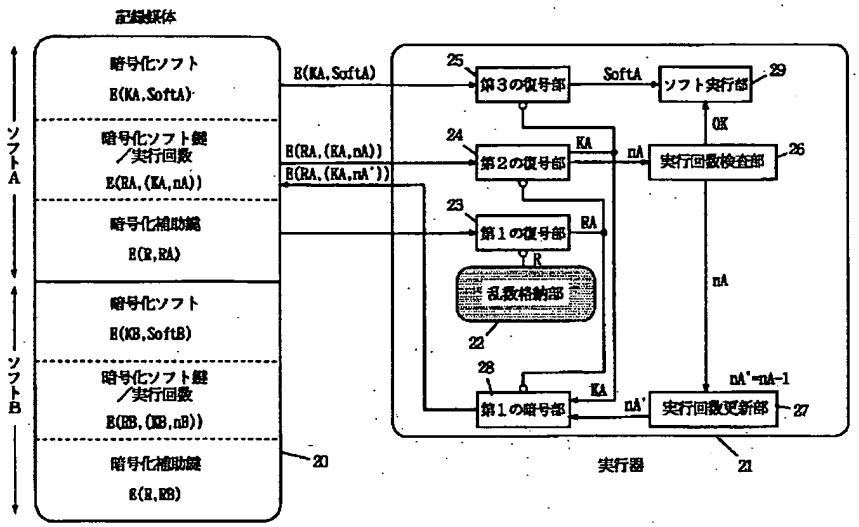
【図2】



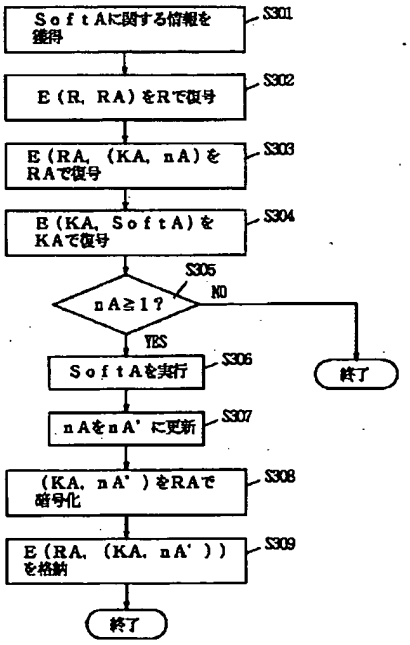
【図3】



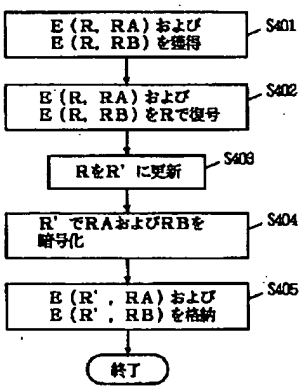
【図5】


記録媒体
ソフトA
ソフトB
暗号化ソフト
E(KA,SoftA)
暗号化ソフト鍵
／実行回数
E(RA,(KA,nA))
暗号化補助鍵
E(R,RA)
暗号化ソフト
E(KB,SoftB)
暗号化ソフト鍵
／実行回数
E(RB,(KB,nB))
暗号化補助鍵
E(R,RB)
20
E(KA,SoftA)
E(RA,(KA,nA))
E(RA,(KA,nA'))
25
第3の復号部
SoftA
ソフト実行部
29
OK
24
第2の復号部
KA
nA
実行回数検査部
26
23
第1の復号部
RA
R
乱数格納部
22
nA
28
第1の暗号部
KA
nA'
nA'=nA-1
実行回数更新部
27
実行器
21

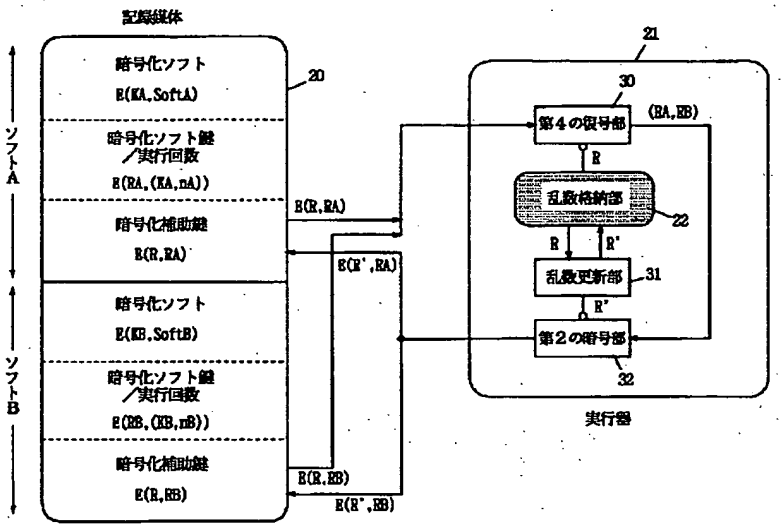
【図6】


ＳｏｆｔＡに関する情報を獲得
S301
Ｅ（Ｒ，ＲＡ）をＲで復号
S302
Ｅ（ＲＡ，（ＫＡ，ｎＡ）をＲＡで復号
S303
Ｅ（ＫＡ，ＳｏｆｔＡ）をＫＡで復号
S304
ｎＡ≧１？
S305
NO
YES
終了
ＳｏｆｔＡを実行
S306
ｎＡをｎＡ'に更新
S307
（ＫＡ，ｎＡ'）をＲＡで暗号化
S308
Ｅ（ＲＡ，（ＫＡ，ｎＡ'））を格納
S309
終了

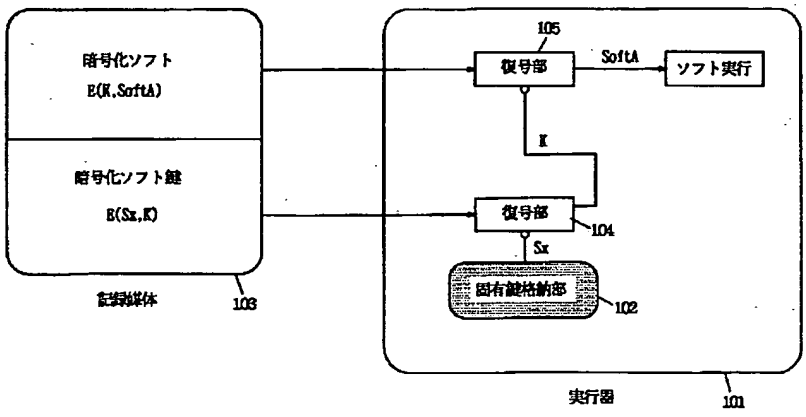
【図8】


Ｅ（Ｒ，ＲＡ）およびＥ（Ｒ，ＲＢ）を獲得
S401
Ｅ（Ｒ，ＲＡ）およびＥ（Ｒ，ＲＢ）をＲで復号
S402
ＲをＲ'に更新
S403
Ｒ'でＲＡおよびＲＢを暗号化
S404
Ｅ（Ｒ'，ＲＡ）およびＥ（Ｒ'，ＲＢ）を格納
S405
終了

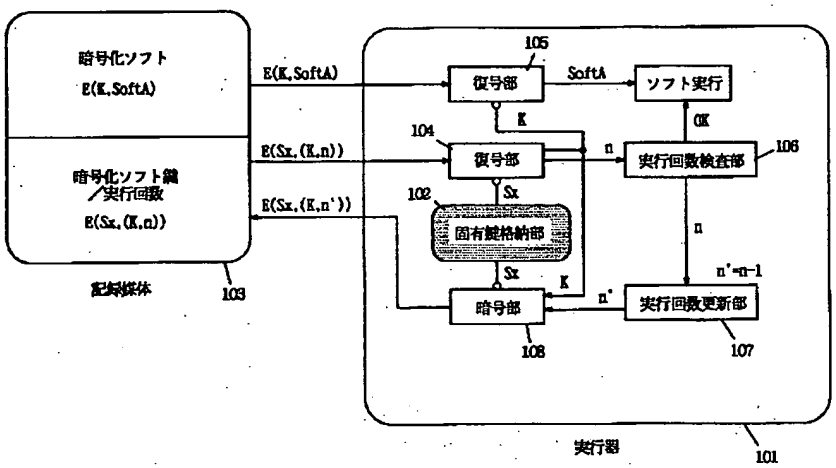
【図7】


記録媒体
暗号化ソフト
E(KA,SoftA)
暗号化ソフト鍵
／実行回数
E(RA,(KA,nA))
暗号化補助鍵
E(R,RA)
暗号化ソフト
E(KB,SoftB)
暗号化ソフト鍵
／実行回数
E(KB,(KB,nB))
暗号化補助鍵
E(R,KB)
ソフトA
ソフトB
20
E(R,RA)
E(R',RA)
E(R,KB)
E(R',KB)
21
30
第4の復号部
(RA,KB)
R
乱数格納部
22
R
R'
乱数更新部
31
R'
第2の暗号部
32
実行器

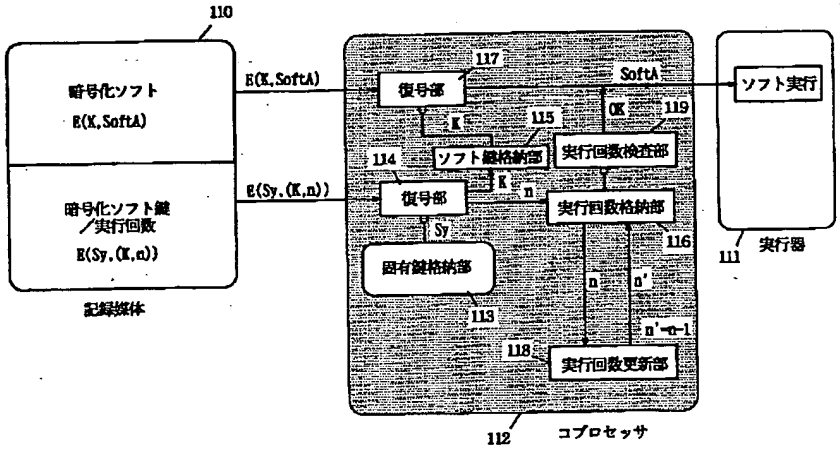
【図9】


暗号化ソフト
E(K,SoftA)
暗号化ソフト鍵
E(Sx,K)
記録媒体
103
105
復号部
SoftA
ソフト実行
K
復号部
104
Sx
固有鍵格納部
102
実行器
101

【図１０】


暗号化ソフト
E(K,SoftA)
暗号化ソフト鍵
／実行回数
E(Sx,(K,n))
記録媒体
103
E(K,SoftA)
E(Sx,(K,n))
E(Sx,(K,n'))
105
復号部
SoftA
ソフト実行
K
OK
104
復号部
n
実行回数検査部
106
Sx
102
固有鍵格納部
n
Sx
K
n'=n-1
暗号部
n'
実行回数更新部
108
107
実行器
101

【図１１】


110
暗号化ソフト
E(K,SoftA)
暗号化ソフト鍵
／実行回数
E(Sy,(K,n))
記録媒体
E(K,SoftA)
E(Sy,(K,n))
117
復号部
SoftA
ソフト実行
K
OK
119
115
ソフト鍵格納部
実行回数検査部
114
K
n
復号部
実行回数格納部
Sy
116
固有鍵格納部
n
n'
113
n'=n-1
118
実行回数更新部
111
実行器
112
コプロセッサ